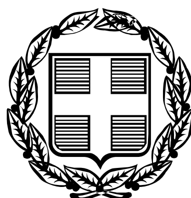


ΕΦΗΜΕΡΙΣ ΤΗΣ ΚΥΒΕΡΝΗΣΕΩΣ

ΤΗΣ ΕΛΛΗΝΙΚΗΣ ΔΗΜΟΚΡΑΤΙΑΣ

ΤΕΥΧΟΣ ΠΡΩΤΟ **Αρ. Φύλλου 59**

20 Μαρτίου 2006

ΑΠΟΦΑΣΕΙΣ

Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης της οργάνωσης και των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων και σχετικές αρμοδιότητες των διοικητικών τους οργάνων.

ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
Ο ΔΙΟΙΚΗΤΗΣ ΤΗΣ ΤΡΑΠΕΖΑΣ ΤΗΣ ΕΛΛΑΔΟΣ
(Πράξη Διοικητή υπ' αριθμ. 2577/9.3.2006)

Αφού έλαβε υπόψη:

α) τον α.ν. 1665/1951, όπως ισχύει, περί ελέγχου και λειτουργίας τραπεζών,

β) το άρθρο 1 του ν. 1266/1982 «Όργανα ασκήσεως της νομισματικής, πιστωτικής και συναλλαγματικής πολιτικής και άλλες διατάξεις»,

γ) τα άρθρα 18, 21 και 22 του ν. 2076/1992 «Ανάληψη και άσκηση δραστηριότητας πιστωτικών ιδρυμάτων και άλλες συναφείς διατάξεις», όπως ισχύουν,

δ) το άρθρο 55Α του Καταστατικού της Τράπεζας της Ελλάδος, που αφορά τις εποπτικές της αρμοδιότητες και την επιβολή κυρώσεων,

ε) τις διατάξεις του ν. 3016/2002 περί της εταιρικής διακυβέρνησης,

στ) τις διατάξεις της ΠΔ/ΤΕ 2438/6.8.1998 για το «Πλαίσιο αρχών λειτουργίας και κριτηρίων αξιολόγησης των Συστημάτων Εσωτερικού Ελέγχου των πιστωτικών ιδρυμάτων και προσδιορισμός αρμοδιοτήτων των οργάνων τους στον τομέα του Εσωτερικού Ελέγχου», όπως αυτή τροποποιήθηκε με τις αποφάσεις της Ε.Τ.Π.Θ. 154/9/18.7.2003 και 193/1/11.3.2005,

ζ) τις διατάξεις της ΠΔ/ΤΕ 2563/19.7.2005, σχετικά με τα στοιχεία που υποβάλλουν τα πιστωτικά ιδρύματα στην Τράπεζα της Ελλάδος για την άσκηση ελέγχου φερεγγυότητας, ρευστότητας και αποδοτικότητας,

η) τις διατάξεις του ν. 2331/1995 όπως τροποποιήθηκε με το ν. 3424/2005 για την πρόληψη της χρησιμοποίησης του χρηματοπιστωτικού συστήματος με σκοπό τη νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες και τη σχετική Εγκύκλιο της Τράπεζας της Ελλάδος 16/2.8.2004,

θ) τη σκοπιμότητα μη επικάλυψης των σχετικών με τα συστήματα εσωτερικού ελέγχου ειδικών ρυθμίσεων (ν. 3016/2002 και σχετική υπ' αριθμ. 2453/30.6.2003 επιστολή της Επιτροπής Κεφαλαιαγοράς),

ι) τη σκοπιμότητα προσαρμογής των αρχών και κριτηρίων που διέπουν τα συστήματα εσωτερικού ελέγχου των πιστωτικών και χρηματοδοτικών ιδρυμάτων προς τις εποπτικής φύσεως εξελίξεις, καθώς και την ανάγκη περαιτέρω εξειδίκευσης επί μέρους θεμάτων ιδίως ως προς τη διαχείριση των κινδύνων και τη συμμόρφωση προς το εκάστοτε ισχύον θεσμικό και κανονιστικό πλαίσιο, αποφασίζουμε:

1. Να καθορίσει τις βασικές γενικές αρχές και κριτήρια, τα οποία θα πρέπει να πληρούνται από κάθε πιστωτικό ίδρυμα και από τα χρηματοδοτικά ιδρύματα, που εποπτεύονται από την Τράπεζα της Ελλάδος, προκειμένου να διασφαλίζεται ότι διαθέτουν, σε ατομικό επίπεδο καθώς και σε επίπεδο ομίλου, αποτελεσματική οργανωτική δομή και επαρκές Σύστημα Εσωτερικού Ελέγχου (ΣΕΕ), που θα περιλαμβάνει τις λειτουργίες Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων και Κανονιστικής Συμμόρφωσης.

2. Να επισημάνει ότι οι βέλτιστες αρχές της εταιρικής διακυβέρνησης αποτελούν αναπόσπαστο τμήμα του ΣΕΕ των πιστωτικών και των χρηματοδοτικών ιδρυμάτων.

3. Η επάρκεια της οργανωτικής δομής και του Συστήματος Εσωτερικού Ελέγχου των πιστωτικών ιδρυμάτων αξιολογούνται από την Τράπεζα της Ελλάδος, με βάση το άρθρο 18 του ν. 2076/1992, όπως εκάστοτε ισχύει, σύμφωνα με τις αρχές που καθορίζονται στην παρούσα Πράξη.

Ι. ΕΙΣΑΓΩΓΗ

Α. Πεδίο εφαρμογής

1. Οι διατάξεις της παρούσας Πράξης εφαρμόζονται:

1.1. Σε όλα τα πιστωτικά ιδρύματα που έχουν έδρα στην Ελλάδα, περιλαμβανομένων των υποκαταστημάτων τους στο εξωτερικό.

1.2. Σε όλα τα χρηματοδοτικά ιδρύματα που λαμβάνουν άδεια λειτουργίας και εποπτεύονται από την Τράπεζα της Ελλάδος σε ατομική βάση. Όλες οι αναφορές των διατάξεων της παρούσας σε πιστωτικά ιδρύματα, που αφορούν υποχρεώσεις σε ατομική βάση, νοούνται, κατά κανόνα και, ως αναφορές στα χρηματοδοτικά ιδρύματα.

2. Σε επίπεδο ομίλου κατά τα ειδικότερα οριζόμενα στο Κεφ. ΙΙΙ «Βασικές αρχές και κριτήρια σε επίπεδο Ομίλου».

3.1. Τα υποκαταστήματα των πιστωτικών ιδρυμάτων με έδρα σε χώρα μέλος του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.) δεν υπόκεινται στο πεδίο εφαρμογής της παρούσας Πράξης, όπως επίσης και τα υποκαταστήματα πιστωτικών ιδρυμάτων με έδρα σε χώρα εκτός του Ε.Ο.Χ., εφόσον έχει αναγνωριστεί από την Τράπεζα της Ελλάδος ότι υπόκεινται σε ισοδύναμο καθεστώς εποπτείας, με βάση τις διατάξεις της ΠΔ/ΤΕ 2461/2000, όπως ισχύει.

3.2. Η πιο πάνω εξαίρεση δεν καλύπτει τις διατάξεις που αφορούν:

3.2.1. Τις διαδικασίες για την πρόληψη και την καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας.

3.2.2. Τις διαδικασίες για τη διασφάλιση της διαφάνειας των συναλλαγών για την επαρκή ενημέρωση των συναλλασσομένων.

3.2.3. Κάθε άλλη υποχρέωση που, με βάση την εκάστοτε ισχύουσα νομοθεσία, επιφυλάσσεται στις αρμοδιότητες της χώρας υποδοχής.

3.3. Τα υποκαταστήματα των αλλοδαπών πιστωτικών ιδρυμάτων γνωστοποιούν στην Τράπεζα της Ελλάδος τις διαδικασίες εσωτερικού ελέγχου που εφαρμόζουν, καθώς και τα συμπεράσματα του ελέγχου της εποπτικής αρχής της χώρας έδρας και των εξωτερικών ελεγκτών σε σχέση με τις δραστηριότητες του υποκαταστήματος που αφορούν τις διατάξεις της ως άνω παρ. 3.2.

Β. Ορισμός και στόχοι Συστήματος Εσωτερικού Ελέγχου

1. Το Σύστημα Εσωτερικού Ελέγχου αποτελεί σύνολο ελεγκτικών μηχανισμών και διαδικασιών που καλύπτει σε συνεχή βάση κάθε δραστηριότητα του πιστωτικού ιδρύματος και συντελεί στην αποτελεσματική και ασφαλή λειτουργία του.

2. Ειδικότερα αποβλέπει στη διασφάλιση των ακόλουθων ιδίως στόχων:

2.1. Τη συνεπή υλοποίηση της επιχειρησιακής στρατηγικής με αποτελεσματική χρήση των διαθέσιμων πόρων.

2.2. Την αναγνώριση και αντιμετώπιση των πάσης φύσεως κινδύνων που αναλαμβάνονται, περιλαμβανομένου και του λειτουργικού κινδύνου.

2.3. Την διασφάλιση της πληρότητας και της αξιοπιστίας των στοιχείων και πληροφοριών που απαιτούνται για τον ακριβή και έγκαιρο προσδιορισμό της χρηματοοικονομικής κατάστασης του πιστωτικού ιδρύματος και την παραγωγή αξιόπιστων οικονομικών καταστάσεων.

2.4. Τη συμμόρφωση με το θεσμικό πλαίσιο που διέπει τη λειτουργία του, περιλαμβανομένων των εσωτερικών κανονισμών και των κανόνων δεοντολογίας.

2.5. Την πρόληψη και την αποφυγή λανθασμένων ενεργειών και παρατυπιών που θα μπορούσαν να θέσουν σε κίνδυνο τη φήμη και τα συμφέροντα του πιστωτικού ιδρύματος, των μετόχων και των συναλλασσομένων με αυτό.

ΙΙ. ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΚΑΙ ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΤΗΣ ΟΡΓΑΝΩΤΙΚΗΣ ΔΟΜΗΣ ΤΟΥ ΣΕΕ

Γενικά

1. Κάθε πιστωτικό ίδρυμα διαθέτει καταγεγραμμένη, τεκμηριωμένη και εγκεκριμένη από το Δ.Σ. Επιχειρησιακή Στρατηγική με χρονικό ορίζοντα τουλάχιστον ενός έτους και σαφείς στόχους, τόσο για το ίδιο πιστωτικό ίδρυμα όσο και για τον όμιλο του οποίου είναι επικεφαλής, που αναφέρεται ιδίως στα ακόλουθα:

1.1. Καταγραφή και ιεράρχηση των άμεσων και μελλοντικών επιχειρησιακών στόχων.

1.2. Διαφανή διάρθρωση και επαρκή τεκμηρίωση της επιχειρηματικής δραστηριότητας στο εσωτερικό και εξωτερικό και κατάλληλες αναφορές που θα καθιστούν δυνατή την κατανόηση της δομής του πιστωτικού ιδρύματος και του ομίλου, τον έλεγχο από τις αρμόδιες εποπτικές αρχές, καθώς και την υλοποίηση της υιοθετηθείσας πολιτικής διαχείρισης κινδύνων σε επίπεδο ομίλου.

1.3. Προϋπολογισμό για το είδος και τον όγκο των δραστηριοτήτων, καθώς και τα προβλεπόμενα οικονομικά αποτελέσματα.

1.4. Τα αποδεκτά όρια και το είδος των κινδύνων που πρόκειται να αναληφθούν, οι παραδοχές με βάση τις οποίες εκτιμώνται και η κάλυψή τους από τα ίδια κεφάλαια.

2. Για την αποτελεσματικότητα του ΣΕΕ ως συνόλου, θα πρέπει να διασφαλίζεται ιδίως ότι:

2.1. Είναι επαρκώς τεκμηριωμένο και λεπτομερώς καταγεγραμμένο ως προς τα σημεία ελέγχου και τις διαδικασίες.

2.2. Είναι κατάλληλα προσαρμοσμένο προς το εύρος, τον όγκο, τους κινδύνους και την πολυπλοκότητα των εργασιών του ιδρύματος, του ομίλου συνολικά και των θυγατρικών, καθώς και προς τις ιδιαιτερότητες των χωρών στις οποίες δραστηριοποιείται.

2.3. Καλύπτει πλήρως όλες τις δραστηριότητες και τις συναλλαγές του πιστωτικού ιδρύματος.

2.4. Παρέχει δυνατότητα ελέγχου των εργασιών των οποίων η διεκπεραίωση ανατίθεται σε άλλες επιχειρήσεις (outsourcing) σύμφωνα με το Παράρτημα 1 της παρούσας Πράξης.

2.5. Υποστηρίζεται από ολοκληρωμένο σύστημα διοικητικών πληροφοριών (MIS) και επικοινωνίας με σαφώς καθορισμένες ιεραρχικές γραμμές αναφοράς που θα επιτρέπουν την έγκαιρη ροή και την αξιοπιστία της απαιτούμενης πληροφόρησης σε κάθε λειτουργό ή διοικητικό όργανο για την εκτέλεση του έργου του.

2.6. Προβλέπει τη διεξαγωγή από τα αρμοδίως επιφορτισμένα όργανα ή μονάδες, περιοδικών ή και έκτακτων ελέγχων, για τη διαπίστωση της συνεπούς εφαρμογής των κανόνων και διαδικασιών από όλες τις υπηρεσιακές μονάδες.

2.7. Διαθέτει εσωτερική συνοχή των μηχανισμών ελέγχου για το σύνολο του πιστωτικού ιδρύματος και του ομίλου του.

2.8. Προβλέπει διαδικασίες για την αξιολόγηση της επάρκειάς του, με κριτήρια:

2.8.1. Τη συνέπεια της εφαρμογής των διαδικασιών.

2.8.2. Τις ποσοτικές και ποιοτικές επιπτώσεις από παραβιάσεις των κανόνων ασφαλείας ή από λάθη και παραλήψεις στην εφαρμογή τους.

2.8.3. Την ύπαρξη μηχανισμών άμεσης αναθεώρησης των διαδικασιών για την αντιμετώπιση των αδυναμιών που διαπιστώνονται από τις τακτικές ή έκτακτες αξιολογήσεις τους.

3. Η Τράπεζα της Ελλάδος θεωρεί ιδιαίτερα χρήσιμη την ανάπτυξη μεθόδων αυτοαξιολόγησης από τις υπηρεσιακές μονάδες, υπό την προϋπόθεση υιοθέτησης καταγεγραμμένων αντικειμενικών κριτηρίων και τελικής

αξιολόγησής τους από τη Μονάδα Εσωτερικής Επιθεώρησης.

Οργανωτική δομή - Διαδικασίες

4. Για τη διασφάλιση αποτελεσματικής οργανωτικής δομής και επάρκειας του ΣΕΕ απαιτείται για κάθε δραστηριότητα αναλυτική περιγραφή και σαφής καθορισμός των αρμοδιοτήτων και ορίων ευθύνης κάθε εμπλεκόμενης υπηρεσιακής μονάδας και Επιτροπής, καθώς και αντίστοιχες διαδικασίες εξουσιοδότησης.

Ειδικότερα απαιτείται:

4.1. Η αναλυτική καταγραφή των διαδικασιών διεξαγωγής κάθε εργασίας, που κοινοποιείται στο αρμόδιο για την εκτέλεση και τον έλεγχό της προσωπικό.

4.2. Η ενσωμάτωση σε όλους τους κανονισμούς διεξαγωγής των εργασιών του πιστωτικού ιδρύματος, κατάλληλων μηχανισμών ελέγχου που θα διασφαλίζουν ότι όλες οι συναλλαγές είναι έγκυρες και νόμιμες, έχουν εκτελεστεί σύμφωνα με όλους τους κανόνες λειτουργίας της κάθε υπηρεσιακής μονάδας, έχουν αξιολογηθεί ως προς τους κινδύνους που ενέχουν, έχουν διεκπεραιωθεί από κατάλληλα εξουσιοδοτημένα και άμεσα εντοπιζόμενα άτομα, έχουν καταχωρηθεί στα προβλεπόμενα για κάθε περίπτωση αρχεία και έχουν ενταχθεί στο σύστημα διοικητικής πληροφόρησης.

4.3. Η πρόβλεψη για άμεση ή έμμεση εμπλοκή δύο τουλάχιστον λειτουργών του πιστωτικού ιδρύματος σε κάθε δραστηριότητα ή ελεγκτική λειτουργία (four eyes principle) μέχρι την ολοκλήρωσή της. Το πιστωτικό ίδρυμα, αξιολογώντας το επίπεδο των κινδύνων, μπορεί κατ' εξαίρεση από τις διατάξεις του προηγούμενου εδαφίου να προβλέπει απλοποιημένες καταγεγραμμένες διαδικασίες για ορισμένες κατηγορίες συναλλαγών, με καθορισμό συγκεκριμένου ορίου συναλλαγών ή και άλλων ποιοτικών χαρακτηριστικών.

4.4. Η συμβουλευτική (τουλάχιστον) συμμετοχή των Μονάδων Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων και Κανονιστικής Συμμόρφωσης στο σχεδιασμό νέων προϊόντων και διαδικασιών σε θέματα που αφορούν στη λήψη επιχειρηματικών αποφάσεων, καθώς και για την εκτίμηση του λειτουργικού κινδύνου που μπορεί να προκύψει, σε περιπτώσεις σημαντικών αλλαγών (συγχωνεύσεις, εξαγορές κ.λπ.), προκειμένου να ενσωματωθούν οι κατάλληλοι ελεγκτικοί μηχανισμοί, οι μηχανισμοί διαχείρισης κινδύνων και να διασφαλισθεί η συμβατότητα με τους ισχύοντες κανόνες.

Θέματα προσωπικού, διαχωρισμού καθηκόντων και σύγκρουσης συμφερόντων

5. Καθορίζονται διαδικασίες διαχείρισης και διαρκούς εκπαίδευσης του ανθρώπινου δυναμικού, έτσι ώστε η στελέχωση κάθε θέσης, εργασίας ή ευθύνης να γίνεται από πρόσωπα που διαθέτουν τις κατάλληλες γνώσεις και ικανότητες με τη θέσπιση των πλέον ενδεδειγμένων εκάστοτε κριτηρίων πρόσληψης και εξέλιξης.

6. Οι αμοιβές των στελεχών και ιδίως αυτών που διαθέτουν προϊόντα και υπηρεσίες ή διαχειρίζονται τα διαθέσιμα κεφάλαια του ιδρύματος διαμορφώνονται με συνεπή συνεκτίμηση της αρχής αποφυγής της παροχής κινήτρων για την ανάληψη υπερβολικών κινδύνων ή τον προσπορισμό βραχυπρόθεσμου οφέλους.

7. Διασφαλίζεται ο αποτελεσματικός διαχωρισμός καθηκόντων με την υιοθέτηση κατάλληλων διαδικασιών, ώστε να αποφεύγονται περιπτώσεις ασυμβίβαστων ρόλων, σύγκρουσης συμφερόντων μεταξύ των μελών του Δ.Σ., της Διοίκησης και των στελεχών, αλλά και μεταξύ αυτών, του πιστωτικού ιδρύματος και των συναλλασσομένων, καθώς και αθέμιτης χρήσης εμπιστευτικών πληροφοριών ή περιουσιακών στοιχείων. Για το σκοπό αυτό λαμβάνονται υπόψη οι βέλτιστες διεθνείς πρακτικές εταιρικής διακυβέρνησης, οι σχετικές διατάξεις της χρηματιστηριακής νομοθεσίας, ο Κώδικας Δεοντολογίας για την παροχή Επενδυτικών Υπηρεσιών, καθώς και οι τυχόν σχετικές αποφάσεις των εποπτικών αρχών.

8. Με κατάλληλες διαφοροποιήσεις στη διοικητική τους υπαγωγή και στις γραμμές διοικητικής αναφοράς διασφαλίζεται η ανεξαρτησία αφενός των οργάνων ελέγχου από τις ελεγχόμενες δραστηριότητες και τους λειτουργούς τους και αφετέρου της διαχείρισης κινδύνων από δραστηριότητες ανάληψης κινδύνων και τους λειτουργούς τους, έτσι ώστε:

8.1. Οι λειτουργίες υποδοχής και διεκπεραίωσης αιτημάτων πελατών, προώθησης και διάθεσης τραπεζικών προϊόντων στο κοινό (πιστώσεις, καταθετικά και επενδυτικά προϊόντα), διαπραγμάτευσης και εν γένει διενέργειας συναλλαγών (front line) να είναι διοικητικά και λειτουργικά διαχωρισμένες από τις λειτουργίες έγκρισης αιτημάτων, επιβεβαίωσης, λογιστικοποίησης και διακανονισμού συναλλαγών, καθώς και φύλαξης τίτλων ή άλλων περιουσιακών στοιχείων του ιδρύματος ή των πελατών.

8.2. Ομοίως, διαχωρισμένες να είναι οι λειτουργίες διαχείρισης κινδύνων και ελέγχου αφενός μεταξύ τους και αφετέρου από τις πιο πάνω λειτουργίες.

9. Διασφαλίζεται ο συστηματικός έλεγχος της πρόσβασης μόνο εξουσιοδοτημένων ατόμων σε περιουσιακά και λογιστικά στοιχεία και εν γένει εμπιστευτικές πληροφορίες.

10. Διασφαλίζεται με κατάλληλες διαδικασίες που θεσπίζονται από το πιστωτικό ίδρυμα, η δυνατότητα πραγματοποίησης ανώνυμων αναφορών, καθώς και η προστασία των υπαλλήλων που μέσω αυτών ενημερώνουν το Δ.Σ. ή την Επιτροπή Ελέγχου (ή όπου αυτή δεν υφίσταται τον εξουσιοδοτημένο υπάλληλο της Μονάδας Εσωτερικής Επιθεώρησης) για σοβαρές παρατυπίες, παραλείψεις ή αξιόποινες πράξεις που υπέπεσαν στην αντίληψή τους.

Συναλλαγές με πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα

11. Ως προς τις συναλλαγές με τα φυσικά ή νομικά πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα, κατά την έννοια της ΠΔ/ΤΕ 2563/19.7.2005, όπως εκάστοτε ισχύει, διασφαλίζεται ότι:

11.1. Υφίσταται λεπτομερής καταγραφή των όρων και διαδικασιών του πιστωτικού ιδρύματος για τις κάθε μορφής πιστοδοτήσεις ή συμμετοχές προς τα πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα, ώστε:

11.1.1. Οι όροι των σχετικών πιστοδοτήσεων να μην αποκλίνουν από τους όρους που εφαρμόζονται στις αντίστοιχες κατηγορίες λοιπών χρηματοδοτήσεων.

11.1.2. Κάθε συμμετοχή ή πιστοδότηση στα πιο πάνω πρόσωπα να πραγματοποιείται μετά από έγκριση του Διοικητικού Συμβουλίου ή απόφαση της Γενικής Συνέλευσης των μετόχων του πιστωτικού ιδρύματος, όπου κατά νόμο απαιτείται.

12.1. Για τη διευκόλυνση της ομαλής χρηματοδοτικής κάλυψης των αναγκών της δραστηριότητας των επι-

χειρήσεων που συμπεριλαμβάνονται στα πρόσωπα που διατηρούν ειδική σχέση με το πιστωτικό ίδρυμα, κατά τα ανωτέρω, το Διοικητικό Συμβούλιο μπορεί να καθορίζει ένα εύλογο όριο πιστοδοτήσεων μέχρι το οποίο δεν απαιτείται η προηγούμενη έγκριση του Δ.Σ., αλλά απλή εκ των υστέρων γνωστοποίηση της αντίστοιχης πιστοδότησης.

12.2. Τα αναφερόμενα στην πιο πάνω παράγραφο πρόσωπα που έχουν ειδική σχέση με το πιστωτικό ίδρυμα γνωστοποιούν στο Διοικητικό Συμβούλιο του πιστωτικού ιδρύματος το σύνολο του υφιστάμενου υπολοίπου των πιστοδοτήσεών τους από συνδεδεμένες με το πιστωτικό - χρηματοδοτικό ίδρυμα επιχειρήσεις, κατά την έννοια του άρθρου 42ε του ν. 2190/1920, όπως ισχύει, εντός 20 ημερών από το τέλος κάθε ημερολογιακού έτους. (Η υποχρέωση αυτή είναι ανεξάρτητη από την υποβολή στοιχείων από το πιστωτικό ίδρυμα στην Τράπεζα της Ελλάδος).

Παρεχόμενες υπηρεσίες προς πελάτες

13. Για τη διασφάλιση της παροχής κατάλληλων υπηρεσιών προς τους πελάτες, ως αναπόσπαστο τμήμα του λειτουργικού κινδύνου, απαιτείται ιδίως:

13.1. Η υιοθέτηση από τα πιστωτικά ιδρύματα των βέλτιστων πρακτικών, για την παροχή υπηρεσιών και προϊόντων που προσιδιάζουν στα χαρακτηριστικά του πελάτη.

13.2. Η παρακολούθηση και αξιολόγηση του τρόπου εξυπηρέτησης και ειδικότερα των διαδικασιών παρουσίασης και συμφωνίας των όρων συνεργασίας τους με το πιστωτικό ίδρυμα, κατά τις εκάστοτε ισχύουσες διατάξεις και ιδίως τη νομοθεσίας περί προστασίας καταναλωτή.

13.3. Η ύπαρξη κατάλληλων διαδικασιών για την εξέταση των καταγγελιών ή παραπόνων των πελατών κατά τις διατάξεις της ΠΔ/ΤΕ 2501/31.10.2002, όπως ισχύει, καθώς και τις λοιπές σχετικές διατάξεις της νομοθεσίας.

13.4. Η διαφύλαξη των συμφερόντων και προστασία από αλλότρια χρήση των προσωπικών δεδομένων. Τα πιστωτικά ιδρύματα θέτουν στη διάθεση της Τράπεζας της Ελλάδος τις άδειες που χορηγούνται από τις αρμόδιες αρχές για την τυχόν χρήση των εν λόγω δεδομένων. Τα περιουσιακά στοιχεία των πελατών να φυλάσσονται και να τηρούνται αναλυτικά και ξεχωριστά από παρόμοια περιουσιακά στοιχεία του πιστωτικού ιδρύματος.

13.5. Ο τακτικός έλεγχος της εφαρμογής των διαδικασιών που σχετίζονται με τη διαπίστωση της ακριβούς ταυτότητας των συναλλασσομένων.

Πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας

14.1. Στο πλαίσιο των υποχρεώσεων σχετικά με την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, υφίστανται κατάλληλη πολιτική και διαδικασίες, όπως εκάστοτε εξειδικεύονται με έγγραφα ή εγκυκλίους της Τράπεζας της Ελλάδος, που θα είναι συνεπείς προς τους στόχους προσέλκυσης πελατείας, τις χώρες δραστηριοποίησης και τα δίκτυα συναλλαγών που χρησιμοποιούν, καθώς και μηχανογραφική υποστήριξη για την αξιολόγηση των πελατών ως προς τους κινδύνους που αντιπροσωπεύουν και την ανάλογη με τον κίνδυνο διαχείρισή τους.

14.2. Υφίστανται διαδικασίες για τον εντοπισμό των συναλλαγών, οι οποίες δεν συνάδουν με την γνώση που έχει το πιστωτικό ίδρυμα για τον πελάτη και τη συναλλακτική του συμπεριφορά, τη διερεύνησή τους και την αναφορά τους, εφόσον απαιτείται, με κατάλληλη τεκμηρίωση και επάρκεια.

14.3. Τα προληπτικού χαρακτήρα μέτρα στον τομέα αυτό πρέπει να διέπονται από τις ίδιες αρχές που εφαρμόζονται σε σχέση με τους λοιπούς κινδύνους και να είναι προσαρμοσμένα στο μέγεθος και τη μορφή του πιστωτικού ιδρύματος. Ειδικότερα να διασφαλίζουν:

14.3.1. Την κατανόηση από τα στελέχη και τις κατά περίπτωση αρμόδιες υπηρεσιακές μονάδες των κινδύνων, κατά κατηγορία πελατών και συναλλαγών ή και σε συνδυασμό τους, καθώς και της πολιτικής και των διαδικασιών που πρέπει να εφαρμόζονται.

14.3.2. Την εφαρμογή κριτηρίων αποδοχής της συμβατικής σχέσης με τον πελάτη, την ταξινόμηση των πελατών κατά βαθμίδα κινδύνου και στη συνέχεια την παρακολούθηση της σχέσης αυτής (δραστηριότητας).

14.3.3. Για την ενίσχυση της αποτελεσματικότητας της πολιτικής να προβλέπεται η, ετήσια αξιολόγηση των μεθοδολογιών και η προσαρμογή της εκπαίδευσης των εξουσιοδοτημένων υπαλλήλων προς τις εκάστοτε νέες συνθήκες και πρακτικές.

Διαχείριση των κινδύνων.

15. Κάθε πιστωτικό ίδρυμα διαθέτει καταγεγραμμένες πολιτική και διαδικασίες που αντιστοιχούν στην Επιχειρησιακή του Στρατηγική, σχετικά με:

15.1. την ανάληψη, την παρακολούθηση και τη διαχείριση των κινδύνων (αγοράς, πιστωτικός, επιτοκίων, ρευστότητας, λειτουργικός κ.λπ.) και τη διάκριση των συναλλαγών και πελατών κατά επίπεδο κινδύνου (όπως χώρα, επάγγελμα, δραστηριότητα),

15.2. τον καθορισμό των εκάστοτε αποδεκτών ανωτάτων ορίων ανάληψης κινδύνου συνολικά για κάθε είδος κινδύνου και περαιτέρω κατανομή καθενός εκ των ορίων αυτών κατά πελάτη, κλάδο, νόμισμα, υπηρεσιακή μονάδα κ.λπ. και

15.3. τη θέσπιση ορίων παύσης ζημιογόνων δραστηριοτήτων ή άλλων διορθωτικών ενεργειών,

που κοινοποιούνται έγκαιρα και εγγράφως, με τη μορφή εξειδικευμένων στόχων ή κατευθύνσεων, όπου απαιτείται, σε όλα τα εντεταλμένα όργανα που εμπλέκονται στις διαδικασίες ανάληψης (risk owners), παρακολούθησης, αντιστάθμισης και μείωσης των κινδύνων.

16. Καθορίζεται η ετήσια επαναξιολόγηση των κινδύνων και προσδιορίζεται ότι οι υψηλού κινδύνου περιοχές, ή οι πολύπλοκες συναλλαγές που καθορίζονται από κάθε πιστωτικό ίδρυμα καθώς και οι προβληματικές πιστοδοτήσεις θα ελέγχονται συχνότερα.

17. Για το σχεδιασμό, την ανάπτυξη και την παρακολούθηση της πολιτικής κινδύνων κάθε πιστωτικό ίδρυμα διαθέτει μια εξειδικευμένη και ανεξάρτητη λειτουργία διαχείρισης των κινδύνων, που καλύπτει όλο το φάσμα των δραστηριοτήτων για όλες τις μορφές των κινδύνων, περιλαμβανομένου του λειτουργικού.

18. Υφίστανται καταγεγραμμένες διαδικασίες ειδικότερα, ως προς:

18.1. Τον περιοδικό εντοπισμό των σημαντικών ή αιφνίδιων μεταβολών στις παραμέτρους που διαμορφώνουν τους κινδύνους (οικονομικά μεγέθη, εξελίξεις στην αγορά, νομικό περιβάλλον κ.λπ.), την αξιολόγησή τους

και την αναφορά τους στα αρμόδια όργανα για τυχόν διορθωτικές ενέργειες, ιδίως όταν οδηγούν σε υπέρβαση των αποδεκτών ορίων.

18.2. Την αντιστάθμιση (κάλυψη, μεταφορά, ασφάλιση) και λογιστικοποίηση της τυχόν ζημιάς.

18.3. Την τιμολόγηση των προσφερόμενων προϊόντων και περιοδική επαναξιολόγησή της, ώστε να διασφαλίζεται ότι λαμβάνονται υπόψη όλες οι παράμετροι διαμόρφωσης του κόστους, ο ανταγωνισμός, οι κίνδυνοι σε σχέση με τις αναμενόμενες αποδόσεις κλπ.

19. Πριν από την επέκταση της δραστηριότητας του πιστωτικού ιδρύματος σε νέα χρηματοπιστωτικά προϊόντα ή υπηρεσίες:

19.1. Θα υπάρχουν τεκμηριωμένες αποφάσεις ενσωμάτωσής τους στη στρατηγική ανάπτυξης του πιστωτικού ιδρύματος.

19.2. Θα έχουν αναγνωρισθεί με ακρίβεια οι σχετικοί κίνδυνοι, συμπεριλαμβανομένου και του λειτουργικού κινδύνου.

19.3. Θα έχει ολοκληρωθεί η ενσωμάτωση των αντίστοιχων ελέγχων και διαδικασιών ή η προσαρμογή των υφιστάμενων στο σύστημα διαχείρισης κινδύνων και εσωτερικού ελέγχου, γενικότερα.

20.1. Κατά τη λήψη επιχειρηματικών αποφάσεων για την ανάληψη σημαντικών κινδύνων (χορήγησης δανείων, αναδιάρθρωσης/ρύθμισης υφιστάμενων δανείων, συμμετοχών, επενδύσεων κ.λπ.), στην περίπτωση κινδύνων που δεν υπόκεινται σε προκαθορισμένες παραμέτρους, καθώς και στον καθορισμό σχετικών ορίων ανάληψης κινδύνων, διασφαλίζεται τουλάχιστον η συμμετοχή της καθ' ύλην αρμόδιας υπηρεσιακής μονάδας και της Μονάδας Διαχείρισης Κινδύνων.

20.2. Στις καταγεγραμμένες και εγκεκριμένες από το Δ.Σ. εσωτερικές διαδικασίες, προσδιορίζεται με πληρότητα ο βαθμός, κατά τον οποίο η λήψη της τελικής απόφασης (ανωτέρω παρ. 20.1.) εξαρτάται από την εισήγηση της Μονάδας Διαχείρισης Κινδύνων. Κατά την αξιολόγηση του συστήματος διαχείρισης κινδύνων κάθε πιστωτικού ιδρύματος, η Τράπεζα της Ελλάδος λαμβάνει θετικά υπόψη την πρόβλεψη κλιμάκωσης της βαρύτητας της εν λόγω εισήγησης ανάλογα με το ύψος και την πολυπλοκότητα των αναλαμβανόμενων κινδύνων (άσκηση βέτο, αυξημένη βαρύτητα, απλός υπολογισμός σε πλειοψηφικό σύστημα κ.λπ.).

20.3. Οι καταγεγραμμένες στα πρακτικά πιο πάνω εισηγήσεις τίθενται, όταν ζητηθούν, υπόψη των αρμόδιων ελεγκτικών οργάνων/υπαλλήλων της Τράπεζας της Ελλάδος, κατά τα προβλεπόμενα στη νομοθεσία (άρθρο 4 του ν.δ. 588/1948 και άρθρο 4 του α.ν. 1665/1951).

Συστήματα λογιστικής παρακολούθησης των εργασιών.

21.1. Από το λογιστικό σύστημα που εφαρμόζει το πιστωτικό ίδρυμα πρέπει γενικά να προκύπτει η πραγματική εικόνα της οικονομικής κατάστασης του πιστωτικού ιδρύματος, να παρέχονται οι απαραίτητες για τη λήψη αποφάσεων πληροφορίες, καθώς και να διασφαλίζεται η κατάρτιση αξιόπιστων ετήσιων ή περιοδικών χρηματοοικονομικών καταστάσεων, σύμφωνα με τα προβλεπόμενα από το νόμο λογιστικά πρότυπα.

21.2. Ειδικότερα, για τη διασφάλιση των ως άνω αρχών, καθώς και την ενίσχυση της συγκρισιμότητας της χρηματοοικονομικής πληροφόρησης και της αποτελεσματικότητας της ασκούμενης εποπτείας, κρίνεται σκόπιμη η εφαρμογή των Διεθνών Λογιστικών Προτύπων από το σύνολο των πιστωτικών ιδρυμάτων.

21.3. Πριν λογιστικοποιηθεί κάθε πράξη είτε ομοειδείς πράξεις ή λογιστικά γεγονότα ελέγχεται από τα αρμόδια όργανα η εγκυρότητα και συμφωνία τους, κατά τα προβλεπόμενα στους σχετικούς εσωτερικούς κανονισμούς του πιστωτικού ιδρύματος. Αξιολογώντας το επίπεδο των κινδύνων, το πιστωτικό ίδρυμα μπορεί κατ' εξαίρεση να καθορίζει συγκεκριμένα όρια συναλλαγών, όπως μικρές ταμειακές συναλλαγές, για τα οποία δεν απαιτείται πρόσθετος έλεγχος πριν τη λογιστικοποίησή τους.

21.4. Κάθε ελεγμένη, κατά τα ανωτέρω, πράξη ή πράξεις καταχωρείται στο λογιστικό σύστημα έγκαιρα, με ακρίβεια και με όλες τις απαραίτητες λεπτομέρειες, σύμφωνα με τα προβλεπόμενα από τα εφαρμοζόμενα λογιστικά πρότυπα και αρχές.

21.5. Τόσο η αρχική αναγνώριση όσο και οι μεταγενέστερες αποτιμήσεις κάθε περιουσιακού στοιχείου ή υποχρέωσης, καθώς και η επίδραση των τελευταίων στα αποτελέσματα ή την καθαρή θέση, θα πραγματοποιούνται με τον τρόπο που προβλέπεται στα ισχύοντα λογιστικά πρότυπα.

21.6. Οι ανοικτές θέσεις από συναλλαγές που ενέχουν κινδύνους αγοράς θα συμφωνούνται τουλάχιστον κάθε μήνα (reconciliation).

21.7. Διασφαλίζεται με κατάλληλες διαδικασίες η συστηματική και ασφαλής τήρηση των αρχείων για χρονικό διάστημα όχι μικρότερο, από τον κατά περίπτωση προβλεπόμενο από το θεσμικό πλαίσιο, ελάχιστο χρόνο και με τρόπο που θα επιτρέπει την πραγματοποίηση ελέγχων μεταγενέστερα (ενσωμάτωση audit trails) και την αναπαραγωγή όλων των συναλλαγών κατά χρονολογική σειρά, την υποστήριξη κάθε καταχωρημένου στοιχείου με πρωτότυπα δικαιολογητικά και την τεκμηρίωση οποιασδήποτε μεταβολής στα υπόλοιπα των λογαριασμών, με αναλυτικά στοιχεία για τις κινήσεις που μεσολάβησαν.

21.8. Διενεργούνται περιοδικοί αλλά και έκτακτοι έλεγχοι επί των διενεργούμενων λογιστικών καταχωρίσεων, ώστε να παρακολουθείται η πιστή εφαρμογή των εγκεκριμένων μεθόδων αποτίμησης των στοιχείων του ισολογισμού και αναγνώρισης του αποτελέσματος.

21.9. Ειδικότερα όσον αφορά τις υποβαλλόμενες στις εποπτικές αρχές οικονομικές πληροφορίες και στοιχεία θα διασφαλίζεται ότι:

21.9.1. Είναι πλήρεις, έγκυρες και βασίζονται σε λογιστικά στοιχεία, και προκειμένου περί εξωλογιστικών υπολογισμών ή εκτιμήσεων, ότι έχουν διενεργηθεί με ορθό και κατάλληλα τεκμηριωμένο τρόπο.

21.9.2. Υποβάλλονται αρμοδίως εντός των καθορισμένων προθεσμιών.

21.10. Υπάρχουν καταγεγραμμένες διαδικασίες για την επιλογή και την απόκτηση του κατάλληλου εξοπλισμού και λογισμικού καθώς και για την επαρκή στελέχωση των αρμοδίων υπηρεσιών, ανάλογα με τις εκάστοτε επιχειρησιακές ανάγκες, τις προοπτικές εξέλιξης του μεγέθους και της φύσης των εργασιών και τις οικονομικές δυνατότητες του πιστωτικού-χρηματοδοτικού ιδρύματος, προκειμένου να διασφαλίζεται, ανά πάσα στιγμή, η επαρκής και αποτελεσματική λογιστική και μηχανογραφική υποστήριξη των εργασιών του.

21.11. Υφίστανται τα απαραίτητα μέσα και εφεδρικά αρχεία δεδομένων, στο πλαίσιο της απαιτούμενης διασφάλισης για τη συνέχιση της επιχειρηματικής δραστη-

ριότητας του πιστωτικού ιδρύματος (Κεφ. IV - ενότητα Α - παρ. 2.8.2.).

21.12. Η Τράπεζα της Ελλάδος αναμένει ότι τα πιστωτικά ιδρύματα θα τηρούν συστήματα που θα διασφαλίζουν την παρακολούθηση, συνολικά, ανά πελάτη, των υπολοίπων και των συναλλαγών που αφορούν ιδίως δάνεια και καταθέσεις, τόσο για την αποτελεσματική διαχείριση κινδύνων, όσο και για την υποβολή των απαιτούμενων στοιχείων προς τις εποπτικές αρχές, το Ταμείο Εγγύησης Καταθέσεων και άλλους φορείς.

Συστήματα πληροφορικής.

22.1. Η λειτουργία των Συστημάτων Πληροφορικής στοχεύει, αφενός στην αποτελεσματική υποστήριξη της επιχειρησιακής στρατηγικής των πιστωτικών ιδρυμάτων, αφετέρου στην ασφαλή διακίνηση, επεξεργασία και αποθήκευση των κρισίμων επιχειρησιακών πληροφοριών. Παράλληλα, η αυξημένη ανάγκη χρήσης συστημάτων πληροφορικής από τα πιστωτικά ιδρύματα, σε συνδυασμό με την τυχόν ανάθεση κρισίμων έργων πληροφορικής σε τρίτους, ενισχύει συγκεκριμένες κατηγορίες κινδύνων με σημαντικότερη αυτή του λειτουργικού κινδύνου. Οι κίνδυνοι αυτοί πρέπει να προσδιορίζονται, να εντοπίζονται έγκαιρα και να αντιμετωπίζονται αποτελεσματικά.

22.2. Στο πλαίσιο της αποτελεσματικής διαχείρισης των κινδύνων που απορρέουν από τη λειτουργία των Συστημάτων Πληροφορικής, τα πιστωτικά ιδρύματα υλοποιούν το πλαίσιο αρχών ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων πληροφορικής που αναφέρεται στο Παράρτημα 2 της παρούσας Πράξης.

Κανονιστική συμμόρφωση.

23.1. Το Δ.Σ. του πιστωτικού ιδρύματος διασφαλίζει την ύπαρξη πολιτικής για την κανονιστική συμμόρφωση και αποτελεσματικού συστήματος εφαρμογής της, που αξιολογούνται από αυτό ετησίως. Η πολιτική κανονιστικής συμμόρφωσης αποσκοπεί:

23.1.1. στην αντιμετώπιση των πάσης φύσεως επιπτώσεων από τυχόν αδυναμία συμμόρφωσης του πιστωτικού ιδρύματος και των εταιρειών του ομίλου του και των επιχειρήσεων προς τις οποίες έχουν εκχωρηθεί δραστηριότητες (Παράρτημα 1 της παρούσας Πράξης) προς το ισχύον νομοθετικό και κανονιστικό πλαίσιο, καθώς επίσης τους κώδικες δεοντολογίας στους οποίους τα πιστωτικά ιδρύματα προσχωρούν και

23.1.2. στη διαχείριση περιπτώσεων σύγκρουσης συμφερόντων. Διευκρινίζεται ότι η αξιολόγηση αυτή δεν επεκτείνεται στην αξιολόγηση της επάρκειας και αποτελεσματικότητας του έργου των καθ' ύλην αρμοδίων μονάδων.

23.2. Για την υλοποίηση της ως άνω πολιτικής θεσπίζεται Λειτουργία ή Μονάδα Κανονιστικής Συμμόρφωσης, κατά τα ειδικότερα αναφερόμενα στο κεφ. V - ενότητα γ.

III. Βασικές αρχές και κριτήρια σε επίπεδο ομίλου.

1. Τα πιστωτικά ιδρύματα οφείλουν να λαμβάνουν όλα τα απαραίτητα μέτρα για την αποτελεσματική ενσωμάτωση στη στρατηγική του ομίλου τους, σχετικά με τα θέματα οργάνωσης και ΣΕΕ, των επιχειρήσεων του χρηματοπιστωτικού τομέα, περιλαμβανομένων των ασφαλιστικών επιχειρήσεων, των οποίων διατηρούν τον έλεγχο, κατά την έννοια του άρθρου 2 του ν. 2076/1992, όπως ισχύει, ή που υπόκεινται σε εποπτεία σε ενοποιημένη βάση σύμφωνα με το π.δ. 267/1995, όπως ισχύει και ενοποιούνται με την ολική ή αναλογική μέθοδο. Ιδιαίτερα θα πρέπει να διασφαλίζεται ότι:

1.1. Τα συστήματα και οι διαδικασίες που εφαρμόζουν οι παραπάνω επιχειρήσεις, καθώς και οι νεοαποκτούμενες επιχειρήσεις (από συγχωνεύσεις, εξαγορές) είναι συμβατά μεταξύ τους και είναι προσαρμοσμένα τόσο στις ανάγκες της οργανωτικής δομής του ομίλου όσο και στις κατ' ιδίαν ιδιαιτερότητες κάθε εταιρείας του ομίλου ή ότι καθορίζεται ρεαλιστικό, κατά περίπτωση, χρονοδιάγραμμα αντίστοιχης προσαρμογής τους.

1.2. Οι σημαντικοί κίνδυνοι στους οποίους εκτίθενται παρακολουθούνται και ελέγχονται σε επίπεδο ομίλου.

1.3. Οι πιο πάνω επιχειρήσεις διαθέτουν επαρκείς διαδικασίες για την παραγωγή και διάθεση των πληροφοριών και στοιχείων που είναι απαραίτητα για την εποπτεία σε ενοποιημένη βάση και για την υλοποίηση των αρμοδιοτήτων που προβλέπονται στις διατάξεις της παρούσας και, ιδίως, για την εφαρμογή των διατάξεων του νέου πλαισίου για την κεφαλαιακή επάρκεια των πιστωτικών ιδρυμάτων (Βασιλεία ΙΙ).

2. Για την ενίσχυση της αποτελεσματικής εφαρμογής των ανωτέρω γενικών αρχών, οι Επιτροπές και οι υπηρεσιακές μονάδες που προβλέπονται στην παρούσα Πράξη ή συστήνονται από τα ίδια τα πιστωτικά ιδρύματα, διατυπώνουν γνώμη για την επιλογή και την καταλληλότητα των επικεφαλής των αντίστοιχων μονάδων των θυγατρικών και αξιολογούν την αποδοτικότητα των μονάδων αυτών.

3. Το Δ.Σ. του μητρικού πιστωτικού ιδρύματος διασφαλίζει, με τον κατάλληλο συντονισμό και συμφωνίες, ότι οι αρμοδιότητες της επίβλεψης και της ενιαίας στρατηγικής δεν αναιρούν τις ευθύνες των διοικητικών οργάνων των θυγατρικών επιχειρήσεων και δεν οδηγούν σε μη απαιτούμενες επικαλύψεις. Επίσης, καθορίζει την κατανομή ευθυνών, τα μέτρα συντονισμού και την ανάθεση, όπου απαιτείται, ειδικών αρμοδιοτήτων σε εταιρίες του ομίλου ως προς τη διαχείριση ιδίως των σημαντικών κινδύνων, τον εσωτερικό έλεγχο, τη λειτουργία κανονιστικής συμμόρφωσης και την εφαρμογή των διατάξεων περί της πρόληψης και καταστολής της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας.

4. Διευκρινίζεται ότι:

4.1. Σε ότι αφορά τις ενοποιούμενες στις οικονομικές καταστάσεις του πιστωτικού ιδρύματος επιχειρήσεις που δεν ανήκουν στο χρηματοπιστωτικό τομέα, θα πρέπει να λαμβάνονται από το πιστωτικό ίδρυμα προσαρμοσμένα αναλόγως μέτρα προκειμένου να διασφαλίζεται σε επίπεδο ομίλου η επίτευξη των στόχων της παρούσας Πράξης.

4.2. Σε περίπτωση που οι ελεγχόμενες από το πιστωτικό ίδρυμα επιχειρήσεις της παρ. 1 είναι εγκατεστημένες εκτός Ελλάδος, τυχόν σημαντική ασυμβατότητα σε επίπεδο ομίλου, που προκύπτει από την αντίστοιχη εφαρμογή των εθνικών διατάξεων της χώρας υποδοχής δεν θα αντιμετωπίζεται, αυτή καθεαυτή, ως παραβίαση των διατάξεων της παρούσας. Όμως, η Τράπεζα της Ελλάδος θα ενημερώνεται από το άμεσα εποπτευόμενο από αυτήν μητρικό πιστωτικό ίδρυμα για τα μέτρα που λαμβάνει για την αντιμετώπιση των πιο πάνω καταστάσεων και θα αξιολογεί την καταλληλότητά τους, ιδίως δε όσων αφορούν τα θέματα πρόληψης και καταστολής της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας.

IV. ΟΡΓΑΝΑ ΔΙΟΙΚΗΤΙΚΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΣΕΕ

Α. Αρμοδιότητες του Διοικητικού Συμβουλίου (Δ.Σ.) και της Διοίκησης.

1. Ανεξάρτητα από την οργανωτική διάρθρωση κάθε πιστωτικού ιδρύματος καθορίζονται τα εξής:

1.1. Το Διοικητικό Συμβούλιο (Δ. Σ.) οφείλει να διαθέτει, ως σύνολο, επαρκείς γνώσεις και εμπειρία τουλάχιστον για τις σημαντικότερες των δραστηριοτήτων του πιστωτικού ιδρύματος, ώστε να έχει τη δυνατότητα άσκησης εποπτείας επί του συνόλου των λειτουργιών είτε άμεσα είτε μέσω των Επιτροπών που θεσμοθετούνται υποχρεωτικά ή κατά τη διακριτική ευχέρεια του πιστωτικού ιδρύματος με βάση την παρούσα Πράξη. Το πιστωτικό ίδρυμα οφείλει να διασφαλίζει τη συμμετοχή στο Δ.Σ. τουλάχιστον ενός ή στην περίπτωση που πληρούται η προϋπόθεση της παρ. 2.2. της ενότητας Β του παρόντος Κεφαλαίου, δύο μη εκτελεστικών και ανεξάρτητων μελών.

Για την αποφυγή περιπτώσεων σύγκρουσης καθηκόντων η Τράπεζα της Ελλάδος κρίνει σκόπιμο τα πιστωτικά ιδρύματα να υιοθετούν τις βέλτιστες διεθνείς πρακτικές και αρχές της εταιρικής διακυβέρνησης που αφορούν, ιδίως, το διαχωρισμό των εκτελεστικών και εποπτικών αρμοδιοτήτων των μελών του Δ.Σ., περιλαμβανομένου του διαχωρισμού των αρμοδιοτήτων του Προέδρου του Διοικητικού Συμβουλίου από τις εκτελεστικές αρμοδιότητες του Διευθύνοντος Συμβούλου.

2. Το Δ.Σ. έχει, γενικά, την ευθύνη για τη συνεπή εφαρμογή των διατάξεων της παρούσας Πράξης και μεταξύ άλλων την ευθύνη:

2.1. Του στρατηγικού προσανατολισμού του πιστωτικού ιδρύματος της επαναξιολόγησής του και της υιοθέτησης κατάλληλων πολιτικών που αποσκοπούν στη διασφάλιση επαρκούς και αποτελεσματικού ΣΕΕ.

2.2. Της ύπαρξης κατάλληλης πολιτικής, τόσο για τη διαχείριση κινδύνων με καθορισμό των εκάστοτε αποδεκτών ανωτάτων ορίων ανάληψης κινδύνου, όσο και για την κανονιστική συμμόρφωση.

2.3. Της διαμόρφωσης του κατάλληλου εσωτερικού περιβάλλοντος, που διασφαλίζει ότι κάθε στέλεχος σε όλα τα ιεραρχικά επίπεδα του πιστωτικού ιδρύματος κατανοεί τόσο τη φύση κάθε κινδύνου που σχετίζεται με τις δραστηριότητες στις οποίες μετέχει ή εποπτεύει, όσο και την ανάγκη της αποτελεσματικής αντιμετώπισής τους, αναγνωρίζει τη σημασία των ελεγκτικών διαδικασιών και διευκολύνει την εφαρμογή τους.

2.4. Της υιοθέτησης Κώδικα Ηθικής Συμπεριφοράς που εφαρμόζεται από τη Διοίκηση και το σύνολο του προσωπικού του πιστωτικού ιδρύματος επί τη βάσει των γενικώς αποδεκτών αρχών (επιμέλεια, αποτελεσματικότητα, υπευθυνότητα, ευπρέπεια στις σχέσεις με το κοινό, μη αίτηση ή αποδοχή ασυνήθους αξίας ωφελημάτων, τήρηση επαγγελματικού απορρήτου κ.λπ.).

2.5. Της παροχής στη Διοίκηση και τις υπηρεσιακές μονάδες όλων των απαραίτητων μέσων για την υλοποίηση του έργου τους.

2.6. Της ακρίβειας των δημοσιευομένων ετήσιων και περιοδικών οικονομικών καταστάσεων του πιστωτικού ιδρύματος και του ομίλου, σε ατομική και ενοποιημένη βάση αντίστοιχα, καθώς και των υποβαλλομένων στην Τράπεζα της Ελλάδος και τις άλλες εποπτικές αρχές στοιχείων.

2.7. Της διασφάλισης ότι η λειτουργία του πιστωτικού ιδρύματος είναι σύμφωνη με τα προβλεπόμενα από το θεσμικό πλαίσιο, τους εσωτερικούς κανονισμούς και τις αρχές της εταιρικής διακυβέρνησης, λαμβάνοντας τα κατάλληλα μέτρα ως προς την επιλογή και τυχόν αντικατάσταση των στελεχών που κατέχουν καίριες θέσεις.

2.8. Της ύπαρξης καταγεγραμμένων διαδικασιών (ανάθεση συγκεκριμένων ρόλων και συντονισμό τους, εξουσιοδοτημένα πρόσωπα για επικοινωνία με την Τράπεζα της Ελλάδος ή και άλλες αρχές, εναλλακτικές πηγές κάλυψης αναγκών ρευστότητας κ.λπ.) που θα διασφαλίζουν:

2.8.1. την αντιμετώπιση εκτάκτων καταστάσεων που θέτουν σε κίνδυνο την ομαλή λειτουργία του πιστωτικού ιδρύματος και

2.8.2. την αποκατάσταση και απρόσκοπτη συνέχιση της επιχειρησιακής του λειτουργίας.

3. Η Διοίκηση, η οποία για τους σκοπούς εφαρμογής της παρούσας Πράξης νοείται ως το ανώτατο διοικητικό όργανο με εκτελεστικές αρμοδιότητες, έχει μεταξύ άλλων την ευθύνη:

3.1. Της συνεπούς υλοποίησης της εγκεκριμένης από το Δ.Σ. επιχειρησιακής στρατηγικής και της εξειδίκευσής της με τη χάραξη κατάλληλης για κάθε λειτουργία πολιτικής, τον καθορισμό επιμέρους στόχων για κάθε τομέα δραστηριότητας, διοικητικό όργανο και υπηρεσιακή μονάδα. Στο πλαίσιο αυτό εντάσσεται και:

3.1.1. Η υλοποίηση της εγκεκριμένης από το Δ.Σ. πολιτικής διαχείρισης κινδύνων.

3.1.2. Ο καθορισμός των επιμέρους ορίων και των αρμοδιοτήτων κάθε υπηρεσιακής μονάδας στη διαχείριση των κινδύνων και η αξιολόγηση της απόδοσής της.

3.1.3. Ο διαρκής έλεγχος της διαχείρισης των κινδύνων του πιστωτικού ιδρύματος μέσα στα εγκεκριμένα από το Δ.Σ. όρια ανάληψης.

3.2. Της ανάπτυξης και ενσωμάτωσης των μηχανισμών και διαδικασιών εσωτερικού ελέγχου, που προσιδιάζουν στο εύρος, το μέγεθος και τη φύση των εργασιών του πιστωτικού ιδρύματος, της περιοδικής αξιολόγησης των σημαντικών, από πλευράς επιπτώσεων, δυσλειτουργιών και της εν γένει αποτελεσματικής εφαρμογής του ΣΕΕ.

Β. Επιτροπές του Δ.Σ. ή της Διοίκησης

1. Γενικοί όροι

1. Ανάλογα με το μέγεθος του πιστωτικού ιδρύματος και την πολυπλοκότητα των εργασιών του, το Δ.Σ. υποβοηθείται στο έργο του από Επιτροπές στις οποίες μπορεί να αναθέτει αρμοδιότητες σχετικά με το ΣΕΕ, προσδιορίζοντας σαφώς τα καθήκοντα, τη σύνθεση και τις διαδικασίες λειτουργίας τους, διασφαλίζοντας σε κάθε περίπτωση την εσωτερική του συνοχή, τη συμπληρωματικότητα και τον απαιτούμενο συντονισμό. Το Δ.Σ. διατηρεί για τις εν λόγω αρμοδιότητες την τελική ευθύνη, εκτός εάν προβλέπεται ρητά από διατάξεις της νομοθεσίας αυξημένος βαθμός ανεξαρτησίας έναντι του Δ.Σ. για συγκεκριμένες αρμοδιότητες (όπως π.χ. της Επιτροπής Ελέγχου), οπότε και γνωστοποιείται στην Τράπεζα της Ελλάδος. Το Δ.Σ. ορίζει από τα μέλη του τον Πρόεδρο των Επιτροπών και καθορίζει τη συχνότητα της περιοδικής εναλλαγής των μελών τους (rotation). Οι σχετικές αποφάσεις καταγράφονται στα πρακτικά του Δ.Σ.

2. Για λόγους ισότητας όρων ανταγωνισμού μεταξύ των πιστωτικών ιδρυμάτων και αποτελεσματικότητας και υπό την επιφύλαξη των παράλληλα ισχυουσών διατάξεων της νομοθεσίας για τη σύσταση Επιτροπών από το Δ.Σ, καθορίζονται τα εξής:

2.1. Συστήνεται υποχρεωτικά από τα πιστωτικά ιδρύματα Επιτροπή Ελέγχου (ενότητα 2α του κεφαλαίου αυτού), εφόσον αυτά:

2.1.1. έχουν εισαγάγει τις μετοχές τους σε οργανωμένη χρηματιστηριακή αγορά ή

2.1.2. διατηρούν θυγατρικές εταιρίες ή υποκαταστήματα στο εξωτερικό ή

2.1.3. το ενεργητικό τους υπερβαίνει το ποσό των 100 εκατ. ευρώ.

2.2. Συστήνεται υποχρεωτικά Επιτροπή Διαχείρισης Κινδύνων (ενότητα 2β του κεφαλαίου αυτού) σε περίπτωση που πληρούται μία από τις προϋποθέσεις των ανωτέρω παρ. 2.1.1 και 2.1.2 του παρόντος κεφαλαίου και το εντός και εκτός ισολογισμού ενεργητικό του πιστωτικού ιδρύματος υπερβαίνει το ποσό των 10 δισ. ευρώ.

Κατ' απόκλιση από τα προαναφερόμενα, το πιστωτικό ίδρυμα μπορεί να αναθέσει, με γνωστοποίηση στην Τράπεζα της Ελλάδος των λόγων που επιβάλουν τη χρήση της εν λόγω δυνατότητας, τις αρμοδιότητες της εν λόγω Επιτροπής τουλάχιστον σε ένα εκτελεστικό και ένα μη εκτελεστικό μέλος του Δ.Σ με επαρκείς γνώσεις και εμπειρία σε θέματα διαχείρισης κινδύνων.

2.3. Δεν απαιτείται η σύσταση της Επιτροπής Διαχείρισης Κινδύνων από το πιστωτικό ίδρυμα στην περίπτωση που τα σχετικά καθήκοντα ασκούνται σε επίπεδο ομίλου από αντίστοιχη Επιτροπή και καλύπτουν ρητά και το πιστωτικό ίδρυμα.

2.4. Λοιπές Επιτροπές.

2.4.1. Τα πιστωτικά ιδρύματα που δεν πληρούν τις ως άνω προϋποθέσεις (παρ. 2.1. και 2.2.) αποφασίζουν για τη σύσταση ανάλογων οργάνων στη βάση της αρχής του κόστους/οφέλους και εν γένει αποτελεσματικότητας, τα οποία και γνωστοποιούνται στην Τράπεζα της Ελλάδος.

2.4.2. Στο πλαίσιο αυτό εντάσσεται και η σύσταση πρόσθετων Επιτροπών, Εκτελεστικής(ών) Επιτροπής(ών) στο επίπεδο της Διοίκησης, η ανάθεση πρόσθετων αρμοδιοτήτων στην Επιτροπή Διαχείρισης Κινδύνων, ή ειδικών αρμοδιοτήτων σε Επιτροπή Διαχείρισης Ενεργητικού Παθητικού (ALCO), Επιτροπή Αμοιβών, κλπ.

2.4.3. Διευκρινίζεται ότι η σύσταση της ειδικής συντονιστικής επιτροπής για την Πληροφορική (I.T. Steering Committee), της οποίας ο Πρόεδρος συνιστάται να είναι μέλος της Διοίκησης, διέπεται από τις διατάξεις του Παραρτήματος 2 (Κεφ. Α1, παρ. 2). Σε ό,τι αφορά την αρμοδιότητα αξιολόγησης της ανάλυσης και διαχείρισης των κινδύνων που σχετίζονται με τα συστήματα πληροφορικής, εναπόκειται στην κρίση του Δ.Σ. η ανάθεσή της στην εν λόγω Επιτροπή ή στην Επιτροπή Διαχείρισης Κινδύνων, όπου υπάρχει.

2. Αρμοδιότητες

α) Επιτροπή Ελέγχου

1.1. Η Επιτροπή Ελέγχου (ΕΕ) ορίζεται από το Δ.Σ. και απαρτίζεται από μη εκτελεστικά μέλη του, κατ' ελάχιστον τρία. Από τα εν λόγω μέλη, το ένα τουλάχιστον είναι ανεξάρτητο, κατά την έννοια του ν. 3016/2002, με επαρκείς γνώσεις και εμπειρία σε λογιστικής και ελεγκτικής φύσεως θέματα.

1.2. Σε περιπτώσεις πιστωτικών ιδρυμάτων που είναι θυγατρικές πιστωτικών ιδρυμάτων (με έδρα στην Ελλάδα ή στο εξωτερικό), η συμμετοχή στην Επιτροπή Ελέγχου εκτελεστικών μελών του Δ.Σ. της μητρικής, υπό την επιφύλαξη της εκάστοτε ισχύουσας νομοθεσίας, δεν έρχεται σε αντίθεση με την ως άνω διάταξη της παρούσας.

2.1. Τα μέλη της Επιτροπής δεν πρέπει να κατέχουν παράλληλες θέσεις ή ιδιότητες ή να διενεργούν συναλλαγές που θα μπορούσαν να θεωρηθούν ασυμβίβαστες με την αποστολή της Επιτροπής. Η συμμετοχή στην Επιτροπή Ελέγχου δεν αποκλείει τη δυνατότητα συμμετοχής και σε άλλες επιτροπές του Δ.Σ.

2.2. Ο Πρόεδρος της Επιτροπής πρέπει να διαθέτει τις απαιτούμενες γνώσεις και εμπειρία για την επίβλεψη των ελεγκτικών διαδικασιών και των λογιστικών θεμάτων που απασχολούν την Επιτροπή ενώ παράλληλα η Επιτροπή Ελέγχου, ως σύνολο, πρέπει να διαθέτει την κατάρτιση και την εμπειρία που απαιτούνται για τη διεκπεραίωση του έργου της, περιλαμβανομένης της γνώσης για το ευρύτερο περιβάλλον λειτουργίας του πιστωτικού ιδρύματος (εντός και εκτός της χώρας) και για τα συστήματα πληροφορικής.

2.3. Η λειτουργία της Επιτροπής Ελέγχου διέπεται από Κανονισμό στον οποίο καθορίζονται η διάρκεια, τα μέλη, η συχνότητα εναλλαγής τους, οι διαδικασίες λήψης των αποφάσεων καθώς και τα κύρια καθήκοντά της, μεταξύ των οποίων συγκαταλέγονται:

2.3.1. Η παρακολούθηση και η ετήσια αξιολόγηση της επάρκειας και αποτελεσματικότητας του Συστήματος Εσωτερικού Ελέγχου σε ατομική βάση και σε επίπεδο ομίλου, εφόσον πρόκειται για μητρική, με βάση τα σχετικά στοιχεία και πληροφορίες της Μονάδας Εσωτερικής Επιθεώρησης, τις διαπιστώσεις και παρατηρήσεις των εξωτερικών ελεγκτών (τακτικών ορκωτών ελεγκτών λογιστών), καθώς και των εποπτικών αρχών.

2.3.2. Η επίβλεψη και η αξιολόγηση των διαδικασιών (βλ. και αρμοδιότητες του Δ.Σ.) κατάρτισης των δημοσιευμένων ετήσιων και, εφόσον συντρέχει σχετική υποχρέωση και, περιοδικών οικονομικών καταστάσεων, του πιστωτικού ιδρύματος και του ομίλου σύμφωνα με τα ισχύοντα λογιστικά πρότυπα.

2.3.3. Η επίβλεψη του διενεργούμενου από τους τακτικούς ορκωτούς ελεγκτές λογιστές ελέγχου των ετήσιων οικονομικών καταστάσεων του πιστωτικού ιδρύματος και η σε τακτική βάση συνεργασία μαζί τους. Στο πλαίσιο της συνεργασίας αυτής, η Επιτροπή ζητά από τους εν λόγω ελεγκτές να αναφέρουν τα τυχόν προβλήματα ή αδυναμίες που εντόπισαν στο ΣΕΕ κατά τον έλεγχο των ετήσιων οικονομικών καταστάσεων σύμφωνα με τα εκάστοτε ισχύοντα Ελληνικά Ελεγκτικά Πρότυπα.

2.3.4. Η υποβολή πρότασης προς το Δ.Σ. για την επιλογή των εξωτερικών ελεγκτών (νοουμένων ως των τακτικών ορκωτών ελεγκτών λογιστών). Η Επιτροπή υποβάλλει επίσης, όποτε το κρίνει σκόπιμο, πρόταση για την αντικατάσταση ή την εναλλαγή τους.

2.3.5. Η διασφάλιση της ανεξαρτησίας, σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία (σήμερα άρθρο 12 ν. 3148/2003) των ορκωτών ελεγκτών λογιστών.

2.3.6. Η υποβολή προτάσεων για την αντιμετώπιση των αδυναμιών που έχουν διαπιστωθεί και η παρακολούθηση της εφαρμογής των μέτρων που αποφασίζονται από το Δ.Σ. (follow up).

2.3.7. Η υποβολή προτάσεων για τις ειδικές περιοχές όπου επιβάλλεται η διενέργεια πρόσθετων ελέγχων από τους εσωτερικούς, ή εξωτερικούς ελεγκτές.

2.3.8. Η αξιολόγηση του έργου της Μονάδας Εσωτερικής Επιθεώρησης με έμφαση σε θέματα που σχετίζονται με το βαθμό ανεξαρτησίας της, την ποιότητα και το εύρος των ελέγχων που διενεργεί, τις προτεραιότητες που προσδιορίζονται από μεταβολές του οικονομικού περιβάλλοντος, των συστημάτων και του επιπέδου των κινδύνων και την εν γένει αποτελεσματικότητα της λειτουργίας της.

3.1. Η Επιτροπή συνεδριάζει τακτικά, τουλάχιστον μία φορά κάθε τρίμηνο, ή και έκτακτα και μπορεί να προσκαλεί μέλη της Διοίκησης και οποιοδήποτε άλλο στέλεχος ή εμπειρογνώμονα, η παρουσία του οποίου, κατά την κρίση της, απαιτείται. Η Επιτροπή τηρεί πρακτικά και ενημερώνει εγγράφως το Δ.Σ. για τα αποτελέσματα του ελεγκτικού της έργου.

3.2. Ο πρόεδρος της Επιτροπής ενημερώνει επίσης το Δ.Σ. για το έργο της Επιτροπής στα πλαίσια των συνεδριάσεων του Δ.Σ.

4.1. Θα ανατίθεται περιοδικά, ύστερα από εισήγηση της Επιτροπής Ελέγχου, τουλάχιστον ανά τριετία, από κάθε πιστωτικό ίδρυμα σε τρίτους, πλην των τακτικών, ορκωτούς ελεγκτές λογιστές που διαθέτουν την απαραίτητη εμπειρία, η αξιολόγηση της επάρκειας του ΣΕΕ σε ατομική και ενοποιημένη βάση, κατά τα ειδικότερα αναφερόμενα στο Παράρτημα 3 της παρούσας Πράξης. Η σχετική έκθεση αξιολόγησης θα γνωστοποιείται στην Τράπεζα της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος) εντός του πρώτου εξαμήνου, μετά από τη λήξη της τριετίας, έτους. Η ελεγκτική εταιρεία και οι ορκωτοί ελεγκτές που αναλαμβάνουν την εργασία αυτή θα εναλλάσσονται, τουλάχιστον, μετά από δύο διαδοχικές αξιολογήσεις.

4.2. Κατά την ανάθεση έργου στους τακτικούς ορκωτούς ελεγκτές λογιστές και τους ορκωτούς ελεγκτές λογιστές που διενεργούν την ανά τριετία αξιολόγηση, θα τους παρέχεται εξουσιοδότηση για την ενημέρωση της Τράπεζας της Ελλάδος, στο πλαίσιο των διατάξεων του άρθρων 18 και 21 του ν. 2076/1992, όπως εκάστοτε ισχύει.

5. Οι πληροφορίες και οι διαπιστώσεις των εξωτερικών ελεγκτών των οικονομικών καταστάσεων του πιστωτικού ιδρύματος θα συζητούνται τριμερώς, μεταξύ του πιστωτικού ιδρύματος, των εξωτερικών ελεγκτών και της Τράπεζας της Ελλάδος, και σε ειδικές περιπτώσεις και διμερώς, μεταξύ των ορκωτών ελεγκτών λογιστών και της Τράπεζας της Ελλάδος (με σχετική ενημέρωση των πιστωτικών ιδρυμάτων), σύμφωνα και με τα οριζόμενα στο εκάστοτε ισχύον Ελληνικό Ελεγκτικό Πρότυπο που αφορά στην επικοινωνία με τις Ρυθμιστικές και Εποπτικές αρχές.

β) Επιτροπή Διαχείρισης Κινδύνων

1.1. Το Δ.Σ. αναθέτει, κατά τα αναφερόμενα στην παρ. 2.2 - ενότητα Β1 του κεφ. IV, τις σχετικές με τη διαχείριση κινδύνων αρμοδιότητες σε Επιτροπή Διαχείρισης Κινδύνων (ΕΔΚ) (ή εναλλακτικά στα δύο μέλη του Δ.Σ. κατά τα προβλεπόμενα στο δεύτερο εδάφιο της παρ. 2.2 - ενότητα Β1 του κεφ. IV), ώστε να καλύπτονται αποτελεσματικά όλες οι μορφές κινδύνων περιλαμβανομένου του λειτουργικού και να διασφαλίζεται ο ενοποιημένος έλεγχός τους, η εξειδικευμένη αντιμετώπισή τους και ο απαιτούμενος συντονισμός σε επίπεδο πιστωτικού ιδρύματος και ομίλου.

1.2. Η Επιτροπή Διαχείρισης Κινδύνων ορίζεται από το Δ.Σ. και απαρτίζεται από μέλη του με επαρκείς γνώσεις και εμπειρία στον τομέα της διαχείρισης κινδύνων, εκ των οποίων ένα τουλάχιστον μέλος είναι εκτελεστικό και ένα μη εκτελεστικό.

2.1. Η λειτουργία της Επιτροπής Διαχείρισης Κινδύνων διέπεται από Κανονισμό στον οποίο καθορίζονται η διάρκεια, τα μέλη, η συχνότητα εναλλαγής τους, οι διαδικασίες λήψης των αποφάσεων καθώς και τα κύρια καθήκοντά της, μεταξύ των οποίων συγκαταλέγονται τουλάχιστον οι ακόλουθες αρμοδιότητες:

2.1.1. Διαμορφώνει τη στρατηγική ανάληψης πάσης μορφής κινδύνων και διαχείρισης κεφαλαίων που ανταποκρίνεται στους επιχειρηματικούς στόχους του πιστωτικού ιδρύματος, σε ατομικό και σε επίπεδο ομίλου και στην επάρκεια των διαθέσιμων πόρων σε τεχνικά μέσα και προσωπικό.

2.1.2. Μεριμνά για την ανάπτυξη εσωτερικού συστήματος διαχείρισης κινδύνων και την ενσωμάτωσή του στη διαδικασία λήψης των επιχειρηματικών αποφάσεων (π.χ. αποφάσεων που αφορούν την εισαγωγή νέων προϊόντων και υπηρεσιών, την προσαρμοσμένη ανάλογα με τον κίνδυνο τιμολόγηση προϊόντων και υπηρεσιών, καθώς και τον υπολογισμό της αποδοτικότητας και την κατανομή κεφαλαίων σε συνάρτηση με τον κίνδυνο) σε όλο το εύρος των δραστηριοτήτων/μονάδων του πιστωτικού ιδρύματος και των θυγατρικών του.

2.1.3. Καθορίζει τις αρχές που πρέπει να διέπουν τη διαχείριση των κινδύνων ως προς την αναγνώριση, πρόβλεψη, μέτρηση, παρακολούθηση, έλεγχο και αντιμετώπισή τους, σε συνέπεια με την εκάστοτε ισχύουσα επιχειρηματική στρατηγική και την επάρκεια των διαθέσιμων πόρων.

2.1.4. Λαμβάνει και αξιολογεί τις υποβαλλόμενες ανά τρίμηνο αναφορές της Μονάδας Διαχείρισης Κινδύνων, ενημερώνει το Δ.Σ. σχετικά με τους σημαντικότερους κινδύνους που έχει αναλάβει το πιστωτικό ίδρυμα και διαβεβαιώνει για την αποτελεσματική αντιμετώπισή τους. Τα πιστωτικά ιδρύματα που δεν υπόκεινται σε σημαντική μεταβολή της διάρθρωσης των δραστηριοτήτων τους μπορούν να εφαρμόσουν διαφορετική συχνότητα αξιολόγησης.

2.2. Σε κάθε περίπτωση όμως, η Επιτροπή Διαχείρισης Κινδύνων αξιολογεί σε ετήσια βάση:

2.2.1. την επάρκεια και την αποτελεσματικότητα της πολιτικής διαχείρισης κινδύνων του πιστωτικού ιδρύματος και του ομίλου του και ιδίως τη συμμόρφωση προς το καθορισμένο επίπεδο ανοχής κινδύνου,

2.2.2. την καταλληλότητα των ορίων, την επάρκεια των προβλέψεων και την εν γένει επάρκεια των ιδίων κεφαλαίων σε σχέση με το ύψος και τη μορφή των αναλαμβανομένων κινδύνων,

τουλάχιστον με βάση την ετήσια έκθεση του επικεφαλής της Μονάδας Διαχείρισης Κινδύνων και του σχετικού απο-

σπάσματος της έκθεσης της Μονάδας Εσωτερικής Επιθεώρησης (Κεφ. V - Ενότητα α - παρ. 2.13.2.β έως και δ).

2.3. Προβλέπει για τη διενέργεια τουλάχιστον ετήσιων προσομοιώσεων καταστάσεων κρίσης (stress tests) για τους κινδύνους αγοράς, πιστωτικό, ρευστότητας και ανάλογων τεχνικών για το λειτουργικό κίνδυνο.

2.4. Διατυπώνει προτάσεις και εισηγείται διορθωτικές ενέργειες στο Δ.Σ. σε περίπτωση που διαπιστώνει αδυναμία υλοποίησης της στρατηγικής που έχει διαμορφωθεί για τη διαχείριση κινδύνων του πιστωτικού ιδρύματος ή αποκλίσεις ως προς την εφαρμογή της.

3. Η Επιτροπή συνεδριάζει τακτικά, τουλάχιστον μία φορά κάθε τρίμηνο, ή και έκτακτα και καλεί οποιοδήποτε μέλος της Διοίκησης ή στέλεχος θεωρεί σκόπιμο. Η Επιτροπή τηρεί πρακτικά και ενημερώνει εγγράφως το Δ.Σ. για τα αποτελέσματα του έργου της.

4. Ο πρόεδρος της Επιτροπής ενημερώνει επίσης το Δ.Σ. για το έργο της Επιτροπής [στα πλαίσια των συνεδριάσεων του Δ.Σ.].

V. ΥΠΗΡΕΣΙΑΚΕΣ ΜΟΝΑΔΕΣ

α. Μονάδα Εσωτερικής Επιθεώρησης

1. Σε όλα τα πιστωτικά ιδρύματα πρέπει να υπάρχει υπηρεσιακή Μονάδα Εσωτερικής Επιθεώρησης (ΜΕΕ), η οποία:

1.1. Είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες και από τις υπηρεσίες που είναι αρμόδιες για την πραγματοποίηση ή λογιστικοποίηση συναλλαγών.

1.2. Αναφέρεται, για τα θέματα αρμοδιότητάς της, στο Δ.Σ. μέσω της Επιτροπής Ελέγχου και στη Διοίκηση, μετά από τον καθορισμό των κατάλληλων προϋποθέσεων που θα διασφαλίζουν την ανεξαρτησία της ΜΕΕ.

2. Στις κύριες αρμοδιότητες της ΜΕΕ εντάσσονται:

2.1. Η διενέργεια ελέγχων προκειμένου να διαμορφωθεί αντικειμενική, ανεξάρτητη και τεκμηριωμένη άποψη για την επάρκεια και την αποτελεσματικότητα του ΣΕΕ, σε επίπεδο πιστωτικού ιδρύματος και του ομίλου του οποίου είναι επικεφαλής.

2.2. Η διενέργεια ειδικών ελέγχων, στις περιπτώσεις που υπάρχουν ενδείξεις για βλάβη των συμφερόντων του πιστωτικού ιδρύματος ή των εταιρειών του ομίλου, με σκοπό τη διεξοδική εξέταση του θέματος και την εξακρίβωση της έκτασης της τυχόν ζημίας.

2.3. Η αξιολόγηση, μέσω των ελέγχων που διενεργεί, του βαθμού εφαρμογής και της αποτελεσματικότητας των διαδικασιών που έχουν θεσπιστεί για τη διαχείριση κινδύνων και τον υπολογισμό των παραμέτρων στις οποίες βασίστηκε η εκτίμηση της κεφαλαιακής επάρκειας του πιστωτικού ιδρύματος και των εταιρειών του ομίλου, όπου προβλέπεται, καθώς και του βαθμού ενσωμάτωσης του συστήματος διαχείρισης κινδύνων στους μηχανισμούς λήψης αποφάσεων (use tests).

2.4. Η επιβεβαίωση προς την Τράπεζα της Ελλάδος της πληρότητας και εγκυρότητας των πιο πάνω διαδικασιών και ειδικότερα των διαδικασιών εκτίμησης των παραμέτρων, στις οποίες βασίστηκε η εκτίμηση του ύψους της πιθανής ζημίας.

2.5. Η αξιολόγηση της οργανωτικής διάρθρωσης, κατανομής αρμοδιοτήτων και καθηκόντων και διαχείριση του ανθρώπινου δυναμικού, καθώς και του βαθμού κατά τον οποίο έχουν καθιερωθεί κατάλληλες πολιτικές και διαδικασίες εταιρικής διακυβέρνησης.

2.6. Η αξιολόγηση του έργου των τομέων εσωτερικού ελέγχου, όπου υπάρχουν, στις μονάδες του πιστωτικού ιδρύματος και των εταιρειών του ομίλου του.

2.7. Η αξιολόγηση της οργάνωσης και λειτουργίας των συστημάτων και μηχανισμών που αφορούν την παραγωγή αξιόπιστης, πλήρους και έγκαιρης χρηματοοικονομικής και διοικητικής πληροφόρησης, όπου αυτή κατά περίπτωση παρέχεται.

2.8. Η αξιολόγηση της οργάνωσης και λειτουργίας των συστημάτων πληροφορικής, κατά τα προβλεπόμενα στο Παράρτημα 2 (Κεφ. Δ), καθώς και των λογιστικών συστημάτων.

2.9. Η αξιολόγηση των διαδικασιών που έχουν θεσπιστεί για την κανονιστική συμμόρφωση.

2.10. Η αξιολόγηση του βαθμού κατά τον οποίο τα συλλογικά όργανα και οι μονάδες του πιστωτικού ιδρύματος καθώς και οι εταιρείες του ομίλου:

2.10.1. Χρησιμοποιούν αποτελεσματικά τα μέσα και τους πόρους που τους διατίθενται για τη συνεπή υλοποίηση της επιχειρησιακής στρατηγικής.

2.10.2. Τηρούν τις κατευθύνσεις και τις διαδικασίες που έχουν αρμοδίως καθορισθεί με στόχο τη συστηματική παρακολούθηση και διαχείριση των πάσης φύσεως κινδύνων που αναλαμβάνονται (π.χ. θέσπιση και τήρηση ορίων).

2.10.3. Μεριμνούν για την διασφάλιση της πληρότητας και ακρίβειας των στοιχείων και πληροφοριών που απαιτούνται για την κατάρτιση αξιόπιστων οικονομικών καταστάσεων, σύμφωνα με τις ισχύουσες λογιστικές αρχές,

2.10.4. Μεριμνούν για την ενσωμάτωση σε όλες τις διαδικασίες και συναλλαγές που διενεργούνται, των κατάλληλων προληπτικών και κατασταλτικών ελεγκτικών μηχανισμών και ασφαλιστικών δικλείδων (controls).

2.11. Η υποβολή προτάσεων για τη θεραπεία τυχόν αδυναμιών που εντοπίζονται στο ΣΕΕ, ή και τη βελτίωση των υφιστάμενων, διαδικασιών και πρακτικών, προκειμένου να επιτυγχάνονται πλήρως οι στόχοι του ΣΕΕ.

2.12. Η παρακολούθηση της εφαρμογής και αποτελεσματικότητας των διορθωτικών μέτρων από τις ελεγχόμενες μονάδες του πιστωτικού ιδρύματος και τις εταιρείες του ομίλου, για την επαρκή αντιμετώπιση των πιο πάνω αδυναμιών και των παρατηρήσεων που καταγράφονται στις εκθέσεις των πάσης φύσεως ελέγχων (εσωτερικών ελεγκτών, εξωτερικών ελεγκτών, εποπτικών αρχών, φορολογικών αρχών κλπ), με σχετική ενημέρωση της Διοίκησης και της Επιτροπής Ελέγχου.

2.13. Η εύλογη και αντικειμενική διαβεβαίωση του Δ.Σ. και της Διοίκησης του πιστωτικού ιδρύματος σχετικά με τη επίτευξη των στόχων του ΣΕΕ, όσον αφορά το πιστωτικό ίδρυμα και τις εταιρείες του ομίλου του οποίου είναι επικεφαλής. Για το σκοπό αυτό η ΜΕΕ:

2.13.1. Ενημερώνει εγγράφως, το Δ.Σ. μέσω της Επιτροπής Ελέγχου και τη Διοίκηση, τουλάχιστον ανά τρίμηνο, καθώς και τις κατά περίπτωση αρμόδιες μονάδες του πιστωτικού ιδρύματος για τις κυριότερες διαπιστώσεις των διενεργούμενων ελέγχων και για τις τυχόν συστάσεις στις οποίες έχει προβεί.

2.13.2. Υποβάλλει, εντός του πρώτου τριμήνου κάθε έτους, στη Διοίκηση και μέσω της Επιτροπής Ελέγχου στο Διοικητικό Συμβούλιο του πιστωτικού ιδρύματος έκθεση σχετικά με:

α) την επάρκεια και αποτελεσματικότητα του ΣΕΕ στο πιστωτικό ίδρυμα και στις εταιρείες του ομίλου,

β) την αποτελεσματικότητα και την τήρηση των διαδικασιών διαχείρισης κινδύνων και των συναφών πιστοδοτικών διαδικασιών, συμπεριλαμβανομένης της πολιτικής προβλέψεων (με επισήμανση των τυχόν μη καλυπτόμενων κινδύνων),

γ) την επάρκεια των διαδικασιών σε σχέση με την εσωτερική αξιολόγηση της κεφαλαιακής επάρκειας του πιστωτικού ιδρύματος,

δ) την εκτίμηση για την πληρότητα της διαδικασίας ή μεθοδολογίας υπολογισμού της απομείωσης της αξίας των δανείων και άλλων περιουσιακών στοιχείων και των τυχόν μεταβολών κατά τη διάρκεια της χρήσης,

καθώς και πρόγραμμα δράσης για τον επόμενο χρόνο.

Το απόσπασμα της έκθεσης που αφορά τις ανωτέρω περιπτώσεις (β) έως και (δ) υποβάλλονται και στην ΕΔΚ (κεφ. IV, ενότητα Β2β, παρ. 2.2.).

Διευκρινίζεται ότι στην ως άνω έκθεση θα περιλαμβάνονται τουλάχιστον οι αντίστοιχες περιοχές/δραστηριότητες που αναφέρονται στο Παράρτημα 3 της παρούσας Πράξης (τριετής έκθεση ελεγκτών λογιστών). Τα τμήματα τουλάχιστον της έκθεσης που αφορούν στις ελεγχόμενες μονάδες θα τους κοινοποιούνται άμεσα για τις διορθωτικές ενέργειές τους.

2.14. Παρέχει στην Τράπεζα της Ελλάδος, κατά κανόνα εγγράφως, οποιαδήποτε στοιχεία ή πληροφορίες ζητηθούν, στο πλαίσιο της ειδικής νομοθεσίας για την εποπτεία των πιστωτικών ιδρυμάτων (νοούμενης ως της πέραν των διατάξεων του ν 3016/2002 νομοθεσίας, του ν.δ. 588/1948, του α.ν. 1965/1951, του ν. 2076/1992 και του άρθρου 55Α του Καταστατικού της Τράπεζας της Ελλάδος), τα οποία αφορούν θέματα της αρμοδιότητάς της και διευκολύνει με κάθε δυνατό τρόπο το έργο της. (Για τις λοιπές εποπτικές αρχές εφαρμόζονται οι διατάξεις του ν. 3016/2002, άρθρο 8).

3. Για την αποτελεσματική άσκηση των αρμοδιοτήτων της, η ΜΕΕ:

3.1. Έχει πρόσβαση σε όλες τις δραστηριότητες και μονάδες, καθώς και σε όλα τα στοιχεία και πληροφορίες του πιστωτικού ιδρύματος και των εταιρειών του ομίλου.

3.2. Διαθέτει έμπειρο και αριθμητικά επαρκές προσωπικό, το οποίο είναι πλήρους και αποκλειστικής απασχόλησης και δεν υπάγεται ιεραρχικά σε άλλη υπηρεσιακή μονάδα του πιστωτικού ιδρύματος. Η Τράπεζα της Ελλάδος δύναται να παρέχει εξαίρεση από την προϋπόθεση της αποκλειστικής απασχόλησης σε ορισμένες κατηγορίες πιστωτικών ιδρυμάτων σύμφωνα με την αρχή της αναλογικότητας.

4. Ο επικεφαλής της ΜΕΕ του πιστωτικού ιδρύματος:

4.1. Ορίζεται από το Διοικητικό Συμβούλιο (κατόπιν εισήγησης της Επιτροπής Ελέγχου, όπου υπάρχει) και η τοποθέτησή του όπως και η τυχόν αντικατάστασή του γνωστοποιούνται στην Τράπεζα της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος). Η Τράπεζα της Ελλάδος διατηρεί την ευχέρεια να ζητήσει την αντικατάστασή του σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια καταλληλότητας ή επάρκειας για την εκπλήρωση των αρμοδιοτήτων του.

4.2. Διαθέτει υψηλού επιπέδου γνώσεις και επαρκή εμπειρία επί ελεγκτικών μεθόδων και των βέλτιστων διεθνών πρακτικών.

4.3. Είναι αποκλειστικής και πλήρους απασχόλησης. Η Τράπεζα της Ελλάδος δύναται να παρέχει εξαίρεση από την υποχρέωση αυτή σε ορισμένες κατηγορίες πιστωτικών ιδρυμάτων, λαμβάνοντας υπόψη την αρχή της αναλογικότητας.

4.4. Μεριμνά για την κατάλληλη οργανωτική δομή της ΜΕΕ, καθώς και για την εφαρμογή εκ μέρους της αποτελεσματικών πολιτικών, διαδικασιών και πρακτικών σύμφωνων με τις βέλτιστες ελεγκτικές πρακτικές και τα πρότυπα του εσωτερικού ελέγχου.

4.5. Ενημερώνει εκ των υστέρων τα αρμόδια όργανα της Τράπεζας της Ελλάδος για σημαντικές μεταβολές σε σχέση με την οργάνωση και λειτουργία της ΜΕΕ.

4.6. Εποπτεύει και συντονίζει τη δραστηριότητα των μονάδων εσωτερικού ελέγχου στις λοιπές μονάδες του πιστωτικού ιδρύματος, εφόσον υφίστανται, και στις εταιρείες του ομίλου.

4.7. Παρίσταται στις Γενικές Συνελεύσεις των Μετόχων του πιστωτικού ιδρύματος.

5. Η Μονάδα Εσωτερικής Επιθεώρησης είναι υπεύθυνη για τον έλεγχο της εφαρμογής των συμφωνηθέντων και την τήρηση των διαδικασιών όσον αφορά την ανάθεση δραστηριοτήτων σε τρίτους (Παράρτημα 1 της παρούσας Πράξης).

β. Μονάδα Διαχείρισης Κινδύνων

1. Σε όλα τα πιστωτικά ιδρύματα θα υπάρχει υπηρεσιακή Μονάδα Διαχείρισης Κινδύνων (ΜΔΚ), η λειτουργία της οποίας θα διέπεται από τις ακόλουθες αρχές:

1.1. Είναι διοικητικά ανεξάρτητη από μονάδες με εκτελεστικές αρμοδιότητες και από τις υπηρεσίες που είναι αρμόδιες για την πραγματοποίηση ή λογιστικοποίηση συναλλαγών και αξιοποιούν την ανάλυση των κινδύνων που διενεργεί.

1.2. Αναφέρεται, για θέματα της αρμοδιότητάς της, στη Διοίκηση και στην Επιτροπή Διαχείρισης Κινδύνων ή και μέσω αυτής στο Δ.Σ.

2. Η ΜΔΚ υπόκειται στον έλεγχο της Μονάδας Εσωτερικής Επιθεώρησης ως προς την επάρκεια και αποτελεσματικότητα των διαδικασιών διαχείρισης κινδύνων.

3. Η ΜΔΚ έχει την ευθύνη για το σχεδιασμό, εξειδίκευση και υλοποίηση της πολιτικής σε θέματα διαχείρισης κινδύνων και κεφαλαιακής επάρκειας, σύμφωνα με τις κατευθύνσεις του Δ.Σ.. Ειδικότερα:

3.1. Χρησιμοποιεί τις κατάλληλες μεθόδους για τη διαχείριση των κινδύνων τους οποίους εν γένει το πιστωτικό ίδρυμα αναλαμβάνει ή στους οποίους μπορεί να εκτεθεί, συμπεριλαμβανομένης της χρήσης υποδειγμάτων (models) για την πρόβλεψη, αναγνώριση, μέτρηση, παρακολούθηση, αντιστάθμιση, μείωση και αναφορά τους.

3.2. Εξειδικεύει (με τη συνεργασία των αρμόδιων εκτελεστικών μονάδων) τα όρια ανάληψης κινδύνων του πιστωτικού ιδρύματος ταυτοποιώντας/καθορίζοντας τις επιμέρους παραμέτρους κατά είδος κινδύνου και ανά κατηγορία αντισυμβαλλομένου, κλάδο, χώρα, νόμισμα, είδος πιστοδοτήσεων, μορφή χρηματοπιστωτικών τίτλων, μετοχών, παραγώγων, επιχειρησιακό χώρο, λειτουργία, δραστηριότητα, προϊόν, σύστημα κλπ και παρακολουθεί την τήρησή τους, θεσπίζοντας τις κατάλληλες διαδικασίες.

3.3. Καθορίζει κριτήρια έγκαιρου εντοπισμού κινδύνων (early warning system) σε ατομικά και συνολικά χαρτοφυλάκια και εισηγείται για τις κατάλληλες διαδικασίες και μέτρα αυξημένης παρακολούθησης, διαρκώς, ή και περιοδικά, αναλόγως της φύσεως των κινδύνων.

3.4. Εισηγείται στην Επιτροπή Διαχείρισης Κινδύνων τις κατάλληλες τεχνικές προσαρμογής των κινδύνων στα αποδεκτά επίπεδα.

3.5. Αξιολογεί περιοδικά την επάρκεια των μεθόδων και συστημάτων αναγνώρισης, μέτρησης και παρακολούθησης κινδύνων και προτείνει διορθωτικά μέτρα εφόσον κριθεί σκόπιμο.

3.6. Διενεργεί ετησίως (με στοιχεία τέλους έτους ή εξαμήνου) δοκιμές προσομοίωσης καταστάσεων κρίσης (stress tests) με σενάρια προσαρμοσμένα στη φύση των δραστηριοτήτων του πιστωτικού ιδρύματος ή/και κατόπιν οδηγιών της Τράπεζας της Ελλάδος για όλες τις μορφές των κινδύνων και ιδίως του πιστωτικού, αγοράς, επιτοκίων και ρευστότητας, αναλύει τα αποτελέσματά τους, εισηγείται τις κατάλληλες πολιτικές και υποβάλλει τα σχετικά αποτελέσματα στην Τράπεζα της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος) εντός τριών (3) μηνών από τη λήξη του έτους ή του εξαμήνου.

3.7. Συντάσσει τις απαιτούμενες για την επαρκή πληροφόρηση της Διοίκησης και του Διοικητικού Συμβουλίου αναφορές σε θέματα της αρμοδιότητάς της, τουλάχιστον ανά τρίμηνο. Τα πιστωτικά ιδρύματα που δεν υπόκεινται σε σημαντική μεταβολή της διάρθρωσης των δραστηριοτήτων τους μπορούν να εφαρμόσουν διαφορετική συχνότητα.

3.8. Προσδιορίζει τις κεφαλαιακές απαιτήσεις και την εν γένει ανάπτυξη μεθοδολογιών εκτίμησής τους για την κάλυψη όλων των κινδύνων στους οποίους εκτίθεται το πιστωτικό ίδρυμα και εισηγείται τις πολιτικές διαχείρισής τους.

4. Για την αποτελεσματική άσκηση των αρμοδιοτήτων της, η ΜΔΚ:

4.1. Έχει πρόσβαση σε όλες τις δραστηριότητες και μονάδες, καθώς και σε όλα τα στοιχεία και πληροφορίες του πιστωτικού ιδρύματος και των εταιρειών του ομίλου, που είναι απαραίτητα για την εκπλήρωση του έργου της.

4.2. Διαθέτει επαρκές, ποσοτικά και ποιοτικά, προσωπικό με εξειδικευμένες γνώσεις, το οποίο είναι πλήρους και αποκλειστικής απασχόλησης.

5. Ο επικεφαλής της Μονάδας Διαχείρισης Κινδύνων:

5.1. Ορίζεται από το Διοικητικό Συμβούλιο (κατόπιν εισήγησης της Επιτροπής Διαχείρισης Κινδύνων, όπου υπάρχει) και η τοποθέτησή του όπως και η τυχόν αντικατάστασή του γνωστοποιούνται στην Τράπεζα της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος). Η Τράπεζα της Ελλάδος διατηρεί την ευχέρεια να ζητήσει την αντικατάστασή του σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια καταλληλότητας ή επάρκειας για την εκπλήρωση των αρμοδιοτήτων του.

5.2. Διαθέτει υψηλού επιπέδου γνώσεις και επαρκή εμπειρία σε θέματα διαχείρισης κινδύνων, τις σχετικές μεθόδους και τις βέλτιστες διεθνείς πρακτικές.

5.3. Συμμετέχει στη διαδικασία λήψης αποφάσεων για τον καθορισμό των όρων των χρηματοδοτήσεων που δεν υπόκεινται σε προκαθορισμένες ή γενικές παραμέτρους.

5.4. Υποβάλλει ετησίως έκθεση στο Δ.Σ., μέσω της ΕΔΚ, σχετικά με τα θέματα που εμπίπτουν στην αρμοδιότητα της ΜΔΚ.

5.5. Συμμετέχει στη διατύπωση εισηγήσεων και προτάσεων άμεσα στη Διοίκηση και μέσω της Επιτροπής Διαχείρισης Κινδύνων στο Δ.Σ. για μεταβολές στη σύνθεση των χαρτοφυλακίων της τράπεζας για την αναδιάρθρωση/ρύθμιση υφιστάμενων δανείων και τη διαφοροποίηση της πολιτικής των προβλέψεων.

5.6. Συμμετέχει στη διαδικασία αξιολόγησης από τις εποπτικές αρχές της επάρκειας του οικονομικού και εποπτικού κεφαλαίου.

5.7. Εποπτεύει και συντονίζει τη δραστηριότητα των μονάδων διαχείρισης κινδύνων, εφόσον υφίστανται, στις λοιπές μονάδες του πιστωτικού ιδρύματος και στις εταιρείες του ομίλου.

γ. Μονάδα Κανονιστικής Συμμόρφωσης

1.1. Στην περίπτωση που το πιστωτικό ίδρυμα πληροί μία από τις προϋποθέσεις των παρ. 2.1.1. και 2.1.2. του Κεφ. IV - ενότητα Β1 - ή το σύνολο των εντός και εκτός ισολογισμού στοιχείων του ενεργητικού του υπερβαίνει το ποσό των € 10 δισεκ., συστήνεται υποχρεωτικά Μονάδα Κανονιστικής Συμμόρφωσης. Εναλλακτικά της υποχρέωσης αυτής, τα εν λόγω πιστωτικά ιδρύματα μπορούν να αναθέτουν τα αντίστοιχα καθήκοντα σε εξουσιοδοτημένους προς τούτο υπαλλήλους, μετά από έγκριση της Τράπεζας της Ελλάδος, η οποία θα αξιολογεί την παροχή της σχετικής δυνατότητας με βάση την πολυπλοκότητα των εργασιών του πιστωτικού ιδρύματος και τους αναλαμβανόμενους από αυτό κινδύνους.

1.2. Στα λοιπά πιστωτικά ιδρύματα τα προαναφερόμενα καθήκοντα εκτελούνται από εξουσιοδοτημένους προς τούτο υπαλλήλους.

2. Η μονάδα (ή τα εξουσιοδοτημένα, κατά τα ανωτέρω πρόσωπα), θα υπάγεται/ονται στη Διοίκηση και θα υποβάλλει/ουν αναφορές, τουλάχιστον ετησίως, για θέματα της αρμοδιότητάς της/τους και στο Δ.Σ.

3. Η εν λόγω μονάδα (ή τα εξουσιοδοτημένα, κατά τα ανωτέρω πρόσωπα) θα είναι διοικητικά ανεξάρτητη/α, θα διασφαλίζεται η αποτροπή σύγκρουσης συμφερόντων κατά την άσκηση των αρμοδιοτήτων της / τους και θα έχει/έχουν τη δυνατότητα απρόσκοπτης πρόσβασης σε όλα τα στοιχεία και πληροφορίες που είναι απαραίτητα για την εκπλήρωση της αποστολής της/τους.

4. Η Μονάδα Κανονιστικής Συμμόρφωσης (ή τα εξουσιοδοτημένα, κατά τα ανωτέρω πρόσωπα) υπόκειται/νται στο έλεγχο της Μονάδας Εσωτερικής Επιθεώρησης ως προς την επάρκεια και αποτελεσματικότητα των διαδικασιών της κανονιστικής συμμόρφωσης.

5. Ως προς τη Μονάδα (ή Λειτουργία) Κανονιστικής Συμμόρφωσης καθορίζονται τα εξής:

5.1. Διευθύνεται από επιλεγμένο πρόσωπο με επαρκείς γνώσεις των τραπεζικών και επενδυτικών δραστηριοτήτων, η τοποθέτηση και η τυχόν αντικατάστασή του οποίου θα γνωστοποιούνται στην ΤτΕ. Η ΤτΕ διατηρεί τη ευχέρεια να ζητήσει την αντικατάσταση του προσώπου αυτού σε περίπτωση που κρίνει ότι δεν πληρούνται τα κριτήρια καταλληλότητας ή επάρκειας για την εκπλήρωση των αρμοδιοτήτων του.

5.2. Έχει ως έργο τη θέσπιση και εφαρμογή κατάλληλων διαδικασιών και την εκπόνηση σχετικού ετήσιου προγράμματος με στόχο να επιτυγχάνεται έγκαιρα η πλήρης και διαρκής συμμόρφωση του πιστωτικού ιδρύματος προς το εκάστοτε ισχύον ρυθμιστικό πλαίσιο και τους εσωτερικούς κανονισμούς του πιστωτικού ιδρύματος και να υφίσταται ανά πάσα στιγμή πλήρης εικόνα για το βαθμό επίτευξης του στόχου αυτού.

5.3. Ενημερώνει τη Διοίκηση και το Δ.Σ. του πιστωτικού ιδρύματος για κάθε διαπιστωθείσα σημαντική παράβα-

ση του κατά τα ως άνω ρυθμιστικού πλαισίου ή τυχόν σημαντικές ελλείψεις.

5.4. Σε περίπτωση τροποποιήσεων του εκάστοτε ισχύοντος ρυθμιστικού πλαισίου, παρέχει σχετικές οδηγίες για την αντίστοιχη προσαρμογή των εσωτερικών διαδικασιών και του εσωτερικού κανονιστικού πλαισίου που εφαρμόζονται από τις υπηρεσιακές μονάδες του πιστωτικού ιδρύματος, καθώς και από τα καταστήματα και τις θυγατρικές εταιρείες εσωτερικού και εξωτερικού. Διασφαλίζει τη διαρκή ενημέρωση των υπαλλήλων για τις εξελίξεις στο σχετικό με τις αρμοδιότητές τους ρυθμιστικό πλαίσιο, με τη θέσπιση κατάλληλων διαδικασιών και εκπαιδευτικών προγραμμάτων.

5.5. Συντονίζει το έργο των υπευθύνων κανονιστικής συμμόρφωσης (compliance officers) των καταστημάτων εξωτερικού του πιστωτικού ιδρύματος και των θυγατρικών εταιρειών εσωτερικού και εξωτερικού, ώστε όλες οι μονάδες να συμμορφώνονται πλήρως με τις ισχύουσες διατάξεις κατά την έννοια του παρόντος κεφαλαίου.

5.6. Διασφαλίζει, με κατάλληλες διαδικασίες, την τήρηση των προθεσμιών για την εκπλήρωση των υποχρεώσεων που προβλέπονται από το κατά τα ως άνω ρυθμιστικό πλαίσιο και παρέχει σχετική διαβεβαίωση προς το Δ.Σ..

5.7. Διασφαλίζει ότι το πιστωτικό ίδρυμα συμμορφώνεται με το κανονιστικό πλαίσιο που σχετίζεται με την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης της τρομοκρατίας.

Ο επικεφαλής μπορεί, κατά την κρίση του πιστωτικού ιδρύματος, και για λόγους αποτελεσματικότητας ή κόστους/οφέλους να αναλαμβάνει και τις ειδικές θεσμικές αρμοδιότητες στον τομέα αυτό κατά τα προβλεπόμενα (ν.2331/1995, όπως τροποποιήθηκε με το ν. 3424/2005, Εγκύκλιος ΤτΕ 16/2.8.2004, όπως εκάστοτε ισχύει), να εισηγείται μέτρα ενίσχυσης της αποτελεσματικότητας της εφαρμογής των υποχρεώσεων και να λειτουργεί ως σημείο επικοινωνίας, για τα θέματα ευθύνης του, με τις αρμόδιες αρχές και τα αρμόδια όργανα της Τράπεζας της Ελλάδος παρέχοντας τις αναγκαίες πληροφορίες.

5.8. Στο πλαίσιο αυτής της αρμοδιότητας καθορίζονται οι κατάλληλες διαδικασίες και τα πρότυπα αναφορών των υπόπτων συναλλαγών προς τις αρμόδιες αρχές, καθώς και οι διαδικασίες για την αμοιβαία πληροφόρηση μεταξύ των υποκαταστημάτων, των θυγατρικών και της μητρικής και παρέχονται οδηγίες για την παύση διενέργειας συναλλαγών που θα έθεταν σε λειτουργικό κίνδυνο το πιστωτικό ίδρυμα.

VI. Υποχρεώσεις γνωστοποίησης στοιχείων

1. Πέραν των ειδικών αναφορών που προβλέπονται στην παρούσα Πράξη (Κεφ.V - ενότητα β - παρ. 3.6.), τα πιστωτικά ιδρύματα υποβάλλουν μέχρι τη λήξη του πρώτου ημερολογιακού εξαμήνου κάθε έτους (ή της τριετίας για την περίπτωση 1.4.) στην Τράπεζα της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος) τις πιο κάτω εκθέσεις, καθώς και τις αντίστοιχες αξιολογήσεις τους από τις αρμόδιες Επιτροπές:

1.1. του ΣΕΕ από τη Μονάδα Εσωτερικής Επιθεώρησης (παρ. 2.13.2. του Κεφ. V - ενότητα α), συμπεριλαμβανομένης της αξιολόγησης των Συστημάτων Πληροφορικής,

1.2. της διαχείρισης κινδύνων από τον επικεφαλής της Μονάδας Διαχείρισης Κινδύνων (σύμφωνα με την παρ. 5.4 του Κεφ.V - ενότητα β),

1.3. των θεμάτων αρμοδιότητας της Μονάδας Κανονιστικής Συμμόρφωσης (παρ. 2 του Κεφ. V - ενότητα γ), καθώς και

1.4. του ΣΕΕ από τους εξωτερικούς ελεγκτές (παρ. 4.1. του Κεφ. IV - ενότητα Β2α και Παράρτημα 3).

2. Διευκρινίζεται ότι οι ως άνω αναφορές δεν υποκαθιστούν τις υποχρεώσεις των πιστωτικών ιδρυμάτων να θέτουν υπόψη των ελεγκτικών οργάνων της Τράπεζας της Ελλάδος, σύμφωνα με τις ειδικές περί πιστωτικών ιδρυμάτων διατάξεις (παρ. 2.14, ενότητα α, Κεφ. V), τα αναγκαία στοιχεία συμπεριλαμβανομένων και των πρακτικών των συζητήσεων σε επίπεδο επιτροπών ή Δ.Σ., επί θεμάτων εσωτερικού ελέγχου και ποιότητας χαρτοφυλακίου, για τη διαπίστωση της τήρησης των υποχρεώσεων της παρούσας, των προϋποθέσεων καταλληλότητας των υπευθύνων προσώπων κατά την εν γένει ισχύουσα νομοθεσία περί εποπτείας.

VII. Εξουσιοδοτήσεις

Εξουσιοδοτείται η Διεύθυνση Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος:

1. να παρέχει οδηγίες και διευκρινίσεις για την εφαρμογή της παρούσας Πράξης και των Παραρτημάτων της,

2. να προσαρμόζει τα ειδικά όρια που προβλέπονται για την εφαρμογή επιμέρους διατάξεων της παρούσας, με κριτήρια που αφορούν το μέγεθος, την πολυπλοκότητα των δραστηριοτήτων και τους αναλαμβανόμενους κινδύνους των πιστωτικών καθώς και των χρηματοδοτικών ιδρυμάτων,

3. να εξειδικεύει, με τη μορφή Παραρτημάτων και Εγκυκλίων, που θα αποτελούν αναπόσπαστο τμήμα της παρούσας Πράξης, τις αρχές και κριτήρια της Πράξης αυτής και προσαρμόζοντάς τα προς την εκάστοτε ισχύουσα νομοθεσία, τις βέλτιστες διεθνείς πρακτικές και εναρμονιστικού χαρακτήρα συστάσεις της Επιτροπής Ευρωπαϊκών Αρχών Τραπεζικής Εποπτείας (CEBS).

4. να καθορίζει, με βάση τα κριτήρια της ανωτέρω παραγράφου 2, την έκταση εφαρμογής επί μέρους διατάξεων της παρούσας από τις συνεταιριστικές τράπεζες και τα χρηματοδοτικά ιδρύματα, θεσπίζοντας, τις κατά περίπτωση κατάλληλες προϋποθέσεις.

VIII. Επιβολή κυρώσεων

Τυχόν παραβίαση διατάξεων της παρούσας Πράξης δύναται να επισύρει την επιβολή από την Τράπεζα της Ελλάδος κυρώσεων, κατά τα προβλεπόμενα στο άρθρο 55Α του Καταστατικού της (άτοκη κατάθεση στην Τράπεζα της Ελλάδος, πρόστιμο υπέρ του Ελληνικού Δημοσίου, διοικητικές κυρώσεις, όπως τα προαναφερόμενα εκάστοτε καθορίζονται με Πράξη του Διοικητή της Τράπεζας της Ελλάδος ή τα εξουσιοδοτημένα από αυτόν όργανα), καθώς και στο άρθρο 22 του ν. 2076/1992.

IX. Λοιπές Διατάξεις

1. Οι διατάξεις της παρούσας Πράξης ισχύουν από 31 Μαίου.2006.

2. Ειδικότερα, για τις διατάξεις της παρούσας που αφορούν:

2.1. Στην υποχρέωση σύστασης Επιτροπής Διαχείρισης Κινδύνων, και Μονάδας (ή θέσπισης λειτουργίας) Κανονιστικής Συμμόρφωσης και

2.2. τις βασικές αρχές και κριτήρια σε επίπεδο Ομίλου (Κεφ. III)

παρέχεται η ευχέρεια εφαρμογής τους από 30 Σεπτεμβρίου2006.

2.3. Στην εφαρμογή των Διεθνών Λογιστικών Προτύπων από το σύνολο των πιστωτικών ιδρυμάτων, ισχύουν από τη χρήση που λήγει την 31.12.2007 (ημερομηνία μετάβασης στα Διεθνή Λογιστικά Πρότυπα 1.1.2006).

3. Από την έναρξη ισχύος των αντίστοιχων διατάξεων της παρούσας:

3.1. Καταργούνται οι διατάξεις της ΠΔ/ΤΕ 2438/6.8.1998, όπως τροποποιήθηκε με τις απόφ. ΕΤΠΘ 154/9/18.7.2003 και 193/1/11.3.2005 και κάθε υφιστάμενη αναφορά σε αυτές νοείται στο εξής ως αναφορά στην παρούσα Πράξη.

3.2. Το Παράρτημα της απόφ. ΕΤΠΘ 193/1/11.3.2005 «Αρχές ασφαλούς και αποτελεσματικής λειτουργίας των συστημάτων πληροφορικής στα πλαίσια της διαχείρισης του λειτουργικού κινδύνου από τα πιστωτικά ιδρύματα», όπως τροποποιείται, προσαρτάται στην παρούσα Πράξη, ως Παράρτημα 2 και αποτελεί στο εξής αναπόσπαστο τμήμα αυτής.

Από τις διατάξεις της Πράξης αυτής δεν προκαλείται δαπάνη σε βάρος του Κρατικού Προϋπολογισμού.

Η Πράξη αυτή να δημοσιευθεί στην Εφημερίδα της Κυβερνήσεως.

Ο Διοικητής

ΝΙΚΟΛΑΟΣ ΓΚΑΡΓΚΑΝΑΣ

Παράρτημα 1

ΑΝΑΘΕΣΗ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ ΣΕ ΤΡΙΤΟΥΣ (OUTSOURCING)

Σύμφωνα με τις διατάξεις της παρ. 2.4 του Κεφ. ΙΙ της παρούσας Πράξης, ως προς την ανάθεση δραστηριοτήτων σε τρίτους, εφαρμόζονται τα εξής:

Α.1. α) Δεν επιτρέπεται από τα πιστωτικά ιδρύματα η ανάθεση σε τρίτους των πιο κάτω υπό στοιχείο 1.1 έως 1.2.6. δραστηριοτήτων.

β) Στην ανωτέρω απαγόρευση δεν εμπίπτουν οι περιπτώσεις, που οι πάροχοι διαθέτουν άδεια και εποπτεύονται για την άσκηση των δραστηριοτήτων αυτών από την Τράπεζα της Ελλάδος, ή την Επιτροπή Κεφαλαιαγοράς ή τις αρμόδιες εποπτικές αρχές χωρών του Ευρωπαϊκού Οικονομικού Χώρου (Ε.Ο.Χ.) ή τρίτων χωρών με ισοδύναμο καθεστώς εποπτείας κατά τις γενικά ισχύουσες διατάξεις.

γ) Στις περιπτώσεις του προηγούμενου εδαφίου απαιτείται μόνον έγκαιρη (τουλάχιστον 20 ημέρες πριν από την υπογραφή της σύμβασης) προηγούμενη γνωστοποίηση στην Τράπεζα της Ελλάδος εκτός από την περίπτωση, κατά την οποία ο πάροχος εδρεύει σε τρίτη (εκτός ΕΟΧ) χώρα, οπότε απαιτείται προηγούμενη σχετική άδεια της Τράπεζα της Ελλάδος, η οποία θα εξετάζεται επί τη βάσει της ισοδυναμίας του εποπτικού πλαισίου και της ευχέρειάς της να έχει πρόσβαση στα στοιχεία ή να διενεργεί τους ελέγχους, που τυχόν απαιτούνται για την άσκηση του εποπτικού της έργου.

1.1.Κύριες τραπεζικές και επενδυτικές δραστηριότητες:

1.1.1. αποδοχή καταθέσεων ή άλλων επιστρεπτέων κεφαλαίων,

1.1.2. χορήγηση πιστώσεων,

1.1.3. πράξεις διενέργειας πληρωμών και μεταφοράς κεφαλαίων,

1.1.4. έκδοση μέσων πληρωμής,

1.1.5. λήψη και διαβίβαση εντολών για λογαριασμό τρίτων,

1.1.6. εκτέλεση εντολών για λογαριασμό τρίτων,

1.1.7. διαπραγμάτευση κινητών αξιών για ίδιο λογαριασμό,

1.1.8. διαχείριση χαρτοφυλακίου για λογαριασμό τρίτων,

1.1.9. αναδοχή και διάθεση κινητών αξιών,

1.2. Παρεπόμενες τραπεζικές και επενδυτικές δραστηριότητες:

1.2.1. πράξεις επί συναλλάγματος, επί χρυσού ή πολύτιμων μετάλλων,

1.2.2. διάθεση, εγγραφή, αγορά διαχείριση φύλαξη και πώληση κινητών αξιών και χρηματοπιστωτικών μέσων,

1.2.3. φύλαξη και διαχείριση χρηματοπιστωτικών μέσων,

1.2.4. παροχή πιστώσεων για την εκτέλεση συναλλαγών επί χρηματοπιστωτικών μέσων,

1.2.5. υπηρεσίες συνδεόμενες με την αναδοχή,

1.2.6. υπηρεσίες συναλλάγματος συνδεόμενες με την παροχή επενδυτικών υπηρεσιών.

2.α) Επιτρέπεται μόνο μετά από προηγούμενη άδεια της Τράπεζας της Ελλάδος, η ανάθεση του συνόλου των αρμοδιοτήτων των Μονάδων Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων, Κανονιστικής Συμμόρφωσης και των πληροφοριακών συστημάτων σε εταιρεία ελεγχόμενη από το πιστωτικό ίδρυμα, κατά την έννοια του άρθρου 2 του ν. 2076/1992, όπως ισχύει.

β) Επίσης άδεια της Τράπεζας της Ελλάδος απαιτείται για την ανάθεση σε επιχείρηση της οποίας το πιστωτικό ίδρυμα δεν διατηρεί τον έλεγχο, επιμέρους καθηκόντων των Μονάδων Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων (π.χ. περιοδική αξιολόγηση συστημάτων διαβάθμισης), Κανονιστικής Συμμόρφωσης και των πληροφοριακών συστημάτων για τη μηχανογραφική υποστήριξη των κύριων δραστηριοτήτων της παρ. 1.

3. Δεν απαιτείται προηγούμενη έγκριση της Τράπεζας της Ελλάδος:

α) όταν οι δραστηριότητες της ανωτέρω παραγράφου (2β) ανατίθενται σε πρόσωπα των οποίων το πιστωτικό ίδρυμα διατηρεί τον έλεγχο. Οι περιπτώσεις αυτές γνωστοποιούνται στην Τράπεζα της Ελλάδος είκοσι (20) τουλάχιστον ημέρες πριν από την υπογραφή της σύμβασης,

β) για τις δραστηριότητες, που δεν εμπίπτουν στις παρ. 1 και 2 ανωτέρω, όπως ενδεικτικά:

- η διαχείριση καρτών (εφόσον δεν συνοδεύεται με παροχή πίστωσης),
- η παροχή νομικών συμβουλών,
- η διαχείριση ανθρώπινου δυναμικού,
- οι διαμεσολαβητικής φύσεως εργασίες (όπως, η προώθηση προϊόντων και υπηρεσιών από πράκτορες του πιστωτικού ιδρύματος, η απλή ειδοποίηση οφειλετών για εξόφληση υποχρεώσεών τους, εκτός εάν συνοδεύεται και με είσπραξη μετρητών οπότε έχουν εφαρμογή οι διατάξεις της παρ. 2 περί παροχής αδείας κ.λπ.).

Στις περιπτώσεις αυτές η Τράπεζα της Ελλάδος θα ενημερώνεται εγγράφως από το πιστωτικό ίδρυμα σε τριμηνιαία βάση, με αρχική ημερομηνία υποβολής την 30.9.2006.

Β.1. Το Διοικητικό Συμβούλιο, η Διοίκηση και τα αρμόδια στελέχη του πιστωτικού ιδρύματος έχουν τη συνολική ευθύνη για τις εργασίες που ανατίθενται σε τρίτους (outsourcing). Στο πλαίσιο αυτό ορίζουν και δια-

σφαλίζουν την τήρηση της σχετικής πολιτικής, η οποία περιλαμβάνει τουλάχιστον τα ακόλουθα:

1.1 Τον προσδιορισμό των δραστηριοτήτων που μπορούν να ανατεθούν σε τρίτους καθώς και τις ανάγκες και τους στόχους που θα εξυπηρετήσει η εν λόγω ανάθεση.

1.2. Την αξιολόγηση των κινδύνων που ενδέχεται να ενέχει η ανάθεση (ή και η τυχόν υποανάθεση) δραστηριοτήτων σε τρίτους και η θέσπιση μηχανισμών για τον έλεγχο των κινδύνων αυτών. Οι παράγοντες που πρέπει να ληφθούν υπόψη κατά την αξιολόγηση του κινδύνου περιλαμβάνουν την κρισιμότητα της ανατιθέμενης δραστηριότητας για το πιστωτικό ίδρυμα, την ύπαρξη εναλλακτικών παροχέων υπηρεσιών για τη συγκεκριμένη δραστηριότητα, το χρόνο και το κόστος που απαιτείται για την ανάληψη της δραστηριότητας εκ νέου από το πιστωτικό ίδρυμα ή τη μεταφορά της σε άλλο πάροχο υπηρεσιών σε περίπτωση αθέτησης της σύμβασης από τον πάροχο (παρ. 1.5.3) και η δυνατότητα ασφαλιστικής κάλυψης για το σύνολο ή μέρος των αναλαμβανόμενων κινδύνων.

1.3. Τις διαδικασίες για την επιλογή του πάροχου υπηρεσιών. Το πιστωτικό ίδρυμα πρέπει να ελέγξει την καταλληλότητα, τη νομιμότητα δραστηριοποίησης, καθώς και την επάρκεια του παρόχου υπηρεσιών όσον αφορά την οικονομική του κατάσταση και τις εφαρμοζόμενες διαδικασίες λειτουργίας και ελέγχου, ώστε να διασφαλίσει ότι ο πάροχος είναι σε θέση να παρέχει το απαιτούμενο επίπεδο υπηρεσιών.

1.4. Τη σύναψη σύμβασης μεταξύ του πιστωτικού ιδρύματος και του παρόχου υπηρεσιών. Η σύμβαση πρέπει να περιγράφει αναλυτικά όλους τους όρους και τις υποχρεώσεις των δύο συμβαλλομένων μερών και να περιλαμβάνει ειδικότερα:

1.4.1. Το σαφή προσδιορισμό της ανατεθείσας δραστηριότητας, της ποιότητας εξυπηρέτησης και απόδοσης καθώς και τις επιπτώσεις από τη μη τήρηση των συμφωνηθέντων. Επίσης, θα καθορίζεται ρητή υποχρέωση του παρόχου ότι θα τηρεί τους κατάλληλους κανόνες συμπεριφοράς και κώδικες δεοντολογίας, καθώς και ότι κατά την εκτέλεση της ανατεθείσας σε αυτόν δραστηριότητας θα λαμβάνεται η κατάλληλη πρόνοια, ώστε να μη δημιουργείται η εντύπωση ότι ο πάροχος ενεργεί για ίδιο λογαριασμό αλλά για λογαριασμό του πιστωτικού ιδρύματος.

1.4.2. Την ανάγκη τήρησης και προστασίας της εμπιστευτικότητας των πληροφοριών που αφορούν τα πιστωτικά ιδρύματα ή / και τους πελάτες τους από σκόπιμη ή ακούσια αποκάλυψή τους σε μη εξουσιοδοτημένα άτομα.

1.4.3. Την περιγραφή των διαδικασιών του εσωτερικού ελέγχου, του σχεδίου έκτακτης ανάγκης καθώς και των λοιπών μέτρων διαχείρισης κινδύνου που υποχρεούται να τηρεί ο πάροχος υπηρεσιών.

1.4.4. Τη δυνατότητα ελεύθερης πρόσβασης του πιστωτικού ιδρύματος στις οικονομικές καταστάσεις, στις εκθέσεις των εσωτερικών και εξωτερικών ελεγκτών καθώς και στα αρχεία του παρόχου υπηρεσιών ή σε οποιεσδήποτε πληροφορίες αφορούν την ανατεθείσα δραστηριότητα.

1.4.5. Τη δυνατότητα της Τράπεζας της Ελλάδος να έχει πρόσβαση στα οικονομικά στοιχεία που αφορούν την εκχωρούμενη δραστηριότητα, καθώς και να διενεργεί επιτόπιους ελέγχους, προκειμένου να διαπιστώσει τη συνεπή τήρηση των συναφών υποχρεώσεων των πιστωτικών ιδρυμάτων προς το ισχύον εποπτικό πλαίσιο και την εν γένει νόμιμη εκτέλεσή τους από τον πάροχο των υπηρεσιών.

1.4.6. Τον τρόπο χειρισμού ενδεχόμενων διαφωνιών, μετατροπών στην αρχική σύμβαση και διακοπής της συνεργασίας μεταξύ του πιστωτικού ιδρύματος και του παρόχου υπηρεσιών.

1.5. Τη θέσπιση ενός συνολικού προγράμματος διαχείρισης του κινδύνου ανάθεσης δραστηριοτήτων σε τρίτους, που θα περιλαμβάνει:

1.5.1. Τη διαρκή παρακολούθηση της οικονομικής κατάστασης του παρόχου υπηρεσιών και των διαδικασιών διεκπεραίωσης των ανατεθεισών σε αυτόν δραστηριοτήτων (με ιδιαίτερη έμφαση στις διαδικασίες ελέγχου και έκτακτης ανάγκης) καθώς και την αξιολόγησή του με βάση προκαθορισμένα ποιοτικά και ποσοτικά κριτήρια. Η Διοίκηση του πιστωτικού ιδρύματος θα προσδιορίσει την καθ' ύλην αρμόδια υπηρεσιακή μονάδα που θα είναι υπεύθυνη για τα ανωτέρω και θα φροντίσει για τη στελέχωσή της με εξειδικευμένο προσωπικό, στο οποίο θα παρέχεται η απαιτούμενη εκπαίδευση. Η εφαρμογή των συμφωνηθέντων καθώς και η τήρηση των σχετικών διαδικασιών θα υπόκειται στον έλεγχο της Μονάδας Εσωτερικής Επιθεώρησης.

1.5.2. Την τήρηση των απαιτούμενων από το πιστωτικό ίδρυμα αρχείων που αφορούν την ανατεθείσα δραστηριότητα στον πάροχο υπηρεσιών, προκειμένου να καθίσταται εφικτός ο έλεγχός τους από τους εσωτερικούς και τους εξωτερικούς ελεγκτές του πιστωτικού ιδρύματος, καθώς και από τις αρμόδιες εποπτικές αρχές.

1.5.3. Την ύπαρξη σχεδίου εκτάκτου ανάγκης, που θα αφορά την εκ νέου ανάληψη της ανατεθείσας δραστηριότητας από το πιστωτικό ίδρυμα ή την ανάθεσή της σε τρίτους, σε περίπτωση που ο πάροχος υπηρεσιών δεν είναι σε θέση να εκπληρώσει τις συμβατικές του υποχρεώσεις, έτσι ώστε να διασφαλιστεί η εύρυθμη λειτουργία του πιστωτικού ιδρύματος.

2. Ενδεχόμενη δυνατότητα υποανάθεσης της εργασίας που, βάσει των ανωτέρω, ανατίθεται αρχικά από το πιστωτικό ίδρυμα σε ανεξάρτητο επαγγελματία ή εταιρεία (chain- outsourcing), επιτρέπεται μόνον εφόσον η σχετική δυνατότητα προβλέπεται στη σύμβαση ανάθεσης που συνάπτει το πιστωτικό ίδρυμα και υπό τον όρο ότι ρητά θα διασφαλίζεται η εκπλήρωση όλων των ανωτέρω προϋποθέσεων υπ' ευθύνη του πιστωτικού ιδρύματος. Στις περιπτώσεις αυτές το πιστωτικό ίδρυμα οφείλει να αξιολογεί και να λαμβάνει ιδιαίτερη μέριμνα για τον κίνδυνο αθέτησης από τον άμεσα αντισυμβαλλόμενο των συμβατικών του υποχρεώσεων, με υπαιτιότητα του τελικού παρόχου της υπηρεσίας.

Παράρτημα 2

ΑΡΧΕΣ ΑΣΦΑΛΟΥΣ ΚΑΙ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗΣ ΛΕΙΤΟΥΡΓΙΑΣ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΠΛΑΙΣΙΑ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΚΙΝΔΥΝΟΥ ΑΠΟ ΤΑ ΠΙΣΤΩΤΙΚΑ ΙΔΡΥΜΑΤΑ

ΕΙΣΑΓΩΓΗ

Το παρόν θέτει ένα δομημένο και λεπτομερές πλαίσιο γενικών αρχών και κριτηρίων για την ασφαλή και αποτελεσματική λειτουργία των Πληροφοριακών Συστη-

μάτων (ΠΣ), λαμβάνοντας παράλληλα υπόψη τις πλέον πρόσφατες εξελίξεις της πληροφορικής στον βαθμό που επηρεάζουν την λειτουργία των Πιστωτικών Ιδρυμάτων (ΠΙ). Το πλαίσιο αποτελεί τη βάση αξιολόγησης των ΠΙ στο συγκεκριμένο τομέα και θα συμβάλλει σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με τα Πληροφοριακά Συστήματα.

Οι αρχές αυτές ομαδοποιούνται σε τέσσερις ενότητες και συγκεκριμένα στις:

• Οργάνωση και Διοίκηση Πληροφορικής, όπου γίνεται αναφορά στην Διακυβέρνηση της Πληροφορικής, στην οργάνωση της Υπηρεσιακής Μονάδας της Πληροφορικής και στις σχέσεις με τους Εξωτερικούς Συνεργάτες.

• Ανάπτυξη και Προμήθεια Συστημάτων, όπου γίνεται αναφορά στις μεθοδολογίες, πρότυπα και διαδικασίες ανάπτυξης και προμήθειας Πληροφοριακών Συστημάτων.

• Λειτουργία και Υποστήριξη, όπου γίνεται αναφορά στις διαδικασίες λειτουργίας των συστημάτων, στη φυσική και λογική τους ασφάλεια, καθώς και στη διασφάλιση της συνέχειας των εργασιών του ΠΙ.

• Έλεγχος Συστημάτων Πληροφορικής, όπου γίνεται αναφορά σε κανόνες και βασικές απαιτήσεις για την επαρκή και αποτελεσματική λειτουργία της Μονάδας Εσωτερικής Επιθεώρησης αναφορικά με τα Πληροφοριακά Συστήματα.

Α. ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΟΙΚΗΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ

Α1. Διακυβέρνηση Πληροφορικής

Η Διακυβέρνηση της Πληροφορικής (Information Technology Governance) είναι ευθύνη της Διοίκησης του ΠΙ. Περιλαμβάνει το σύνολο των κατάλληλων επιχειρησιακών δομών και διαδικασιών μέσω των οποίων διασφαλίζεται ότι η Πληροφορική υποστηρίζει τη στρατηγική και τους στόχους του ΠΙ, διαχειρίζεται αποτελεσματικά τους πόρους που της διατίθενται, αξιολογεί και διαχειρίζεται αποτελεσματικά τους κινδύνους που απορρέουν από την λειτουργία των Πληροφοριακών Συστημάτων, εφαρμόζει πιστά την Πολιτική Ασφάλειας, είναι σε θέση να μετρήσει την αποτελεσματικότητα και αποδοτικότητά της και τέλος υλοποιεί ένα σύνολο μηχανισμών ελέγχου στα πλαίσια ενός γενικότερου ελεγκτικού πλαισίου.

Για την επίτευξη των προαναφερθέντων το ΠΙ θα πρέπει:

1. να διαθέτει καταγεγραμμένη και εγκεκριμένη στρατηγική για την Πληροφορική, συμβατή με τη γενικότερη επιχειρησιακή στρατηγική του. Η στρατηγική της Πληροφορικής οφείλει, αφενός μεν να υλοποιεί τους επιχειρησιακούς στόχους που έχουν τεθεί από τη Διοίκηση του ΠΙ, αφετέρου δε να διαμορφώνει έγκαιρα την απαραίτητη τεχνολογική υποδομή για τις μελλοντικές ανάγκες του οργανισμού. Το ΠΙ πρέπει να διαθέτει τα κατάλληλα υπηρεσιακά όργανα και διαδικασίες για τη χάραξη της στρατηγικής της Πληροφορικής, την τήρηση και την περιοδική ενημέρωσή της, ώστε να εναρμονίζεται διαρκώς με τους εκάστοτε επιχειρησιακούς στόχους και το εκάστοτε ισχύον θεσμικό πλαίσιο. Η εγκεκριμένη στρατηγική της Πληροφορικής πρέπει να περιλαμβάνει τόσο βραχυπρόθεσμα (ετήσια) όσο και μέσο - μακροπρόθεσμα (τριετή) σχέδια.

2. να διαθέτει Ειδική Συντονιστική Επιτροπή για την Πληροφορική (I.T. Steering Committee). Επικεφαλής της επιτροπής συνιστάται να είναι μέλος της Διοίκησης με γνώση των θεμάτων πληροφορικής και μέλη διευθυντικά στελέχη του οργανισμού. Ο ρόλος, τα καθήκοντα και η ελάχιστη σύνθεση της Επιτροπής θα πρέπει να ορίζονται σε επίσημο κανονισμό. Στα καθήκοντα της Επιτροπής, μεταξύ άλλων, περιλαμβάνονται:

• η αξιολόγηση των βραχυπρόθεσμων και μέσο-μακροπρόθεσμων σχεδίων της Πληροφορικής στα πλαίσια της επιχειρησιακής στρατηγικής,

• η αξιολόγηση της Ανάλυσης και Διαχείρισης των Κινδύνων που σχετίζονται με τα Πληροφοριακά Συστήματα,

• η αξιολόγηση και έγκριση μεγάλων προμηθειών υλικού και λογισμικού,

• η εποπτεία των μεγάλων έργων και του προϋπολογισμού της Πληροφορικής,

• ο καθορισμός προτεραιοτήτων,

• η αξιολόγηση πολιτικών, προτύπων και διαδικασιών,

• η έγκριση και εποπτεία των συνεργασιών με τρίτους (π.χ. θέματα outsourcing).

Η Επιτροπή, τέλος, θα πρέπει να λαμβάνει γνώση των πορισμάτων των ελέγχων που διενεργούνται στα Πληροφοριακά Συστήματα.

3. να αξιολογεί, κατηγοριοποιεί και διαχειρίζεται τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία των Πληροφοριακών Συστημάτων. Οι κίνδυνοι αυτοί θα πρέπει να συνεκτιμούνται με τους υπόλοιπους κινδύνους στους οποίους είναι εκτεθειμένο το ΠΙ.

4. να διαθέτει καταγεγραμμένη και εγκεκριμένη από την Διοίκηση Πολιτική Ασφάλειας για τα Πληροφοριακά Συστήματα με τη μορφή αρχών - δεσμεύσεων, οι οποίες θα προδιαγράφουν τις κατευθύνσεις και τους στόχους του οργανισμού για την αποτελεσματική διαχείριση, προστασία και κατανομή των πληροφοριακών του πόρων. Η Πολιτική Ασφάλειας οφείλει:

(i) να παραπέμπει σε συγκεκριμένα πρότυπα και διαδικασίες δεσμεύοντας έτσι τις υπηρεσιακές μονάδες στην υλοποίηση και το προσωπικό στην τήρησή τους,

(ii) να προσφέρει ένα κανονιστικό πλαίσιο βάσει του οποίου διενεργούνται οι έλεγχοι και

(iii) να προσαρμόζεται και ενημερώνεται βάσει θεσμοθετημένων διαδικασιών.

Το περιεχόμενο της Πολιτικής Ασφάλειας θα πρέπει να κοινοποιείται στο προσωπικό του ΠΙ και να υπάρχει από αυτό η έγγραφη αποδοχή του. Η ύπαρξη της Πολιτικής Ασφάλειας, οι στόχοι της, η σύνοψή της, και το περιεχόμενο συγκεκριμένων τμημάτων της -αν αυτό απαιτείται-, μπορεί να γνωστοποιείται στο κοινό, έτσι ώστε να προάγεται το αίσθημα εμπιστοσύνης των πελατών απέναντι στο ΠΙ.

5. να διαθέτει, πέραν της Πολιτικής Ασφάλειας, την κατάλληλη διοικητική δομή που θα εγγυάται τη ασφάλεια των επιχειρησιακών πληροφοριών. Στο πλαίσιο αυτής της δομής θα πρέπει τουλάχιστον να προβλέπεται θέση Υπεύθυνου Ασφάλειας ΠΣ, η αμεροληψία και η ανεξαρτησία του οποίου θα πρέπει να διασφαλίζονται μέσω της απευθείας αναφοράς του σε υψηλά κλιμάκια της ιεραρχίας.

6. να μεριμνά ώστε οι υπάρχουσες πολιτικές, πρότυπα, διαδικασίες και μεθοδολογίες να είναι επίσημα καταγεγραμμένες και εγκεκριμένες από τα αρμόδια υπηρεσιακά όργανα.



7. να διαθέτει πρότυπα και μεθοδολογίες για το σχεδιασμό και την ανάπτυξη των Πληροφοριακών Συστημάτων, καθώς και διαδικασίες για την καθημερινή τους λειτουργία και υποστήριξη.

8. να διαθέτει πρότυπα και διαδικασίες για τη διαχείριση των έργων πληροφορικής. Στην πρόταση για την υλοποίηση κάθε μεγάλου έργου πληροφορικής πρέπει να προσδιορίζεται ο επιχειρησιακός στόχος, καθώς και τα ποιοτικά και ποσοτικά οφέλη που θα αποφέρει η υλοποίησή του. Η αποτελεσματική έκβαση ενός έργου διασφαλίζεται με την ύπαρξη και τήρηση καταλλήλων μεθοδολογιών και πρακτικών που ακολουθούνται σε όλο τον κύκλο ζωής του. Σε αυτές περιλαμβάνονται, μεταξύ άλλων, η μεθοδολογία και τα εργαλεία παρακολούθησης του έργου, ο συντονισμός των απαιτούμενων ενεργειών και πόρων, η τήρηση χρονοδιαγραμμάτων, η παρακολούθηση του κόστους, η συμμετοχή των στελεχών τόσο της Πληροφορικής όσο και των άλλων επιχειρησιακών μονάδων στις διάφορες φάσεις υλοποίησης, η μεθοδολογία διαχείρισης αλλαγών, η εκπαίδευση του προσωπικού. Τέλος, η διασφάλιση της ποιότητας πρέπει να αποτελεί ανεξάρτητη διαδικασία στην οργάνωση και διαχείριση ενός έργου πληροφορικής.

9. να εγγυάται την ποιότητα των παρεχόμενων υπηρεσιών πληροφορικής μέσω της ύπαρξης διαδικασιών διασφάλισης ποιότητας και εναρμόνισης με τα πρότυπα ποιότητας που έχει θέσει το ΠΙ. Η ποιότητα πρέπει να διασφαλίζεται σε όλα τα στάδια του κύκλου ζωής των συστημάτων και να καλύπτει τα παραδοτέα, την τεκμηρίωση, την εκπαίδευση, τις προδιαγραφές, τις διαδικασίες, και τα σχέδια υλοποίησης ενός έργου.

10. να διαθέτει τις κατάλληλες διαδικασίες για τον έγκαιρο εντοπισμό και την αποτελεσματική αντιμετώπιση των προβλημάτων που προκύπτουν στα Πληροφοριακά Συστήματα.

11 να διαθέτει διαδικασίες καταγραφής και κατηγοριοποίησης των γεγονότων που δημιουργούν λειτουργικό κίνδυνο, συμπεριλαμβανομένων των ζημιών (detailed event type logging and classification) που προέρχονται από προβλήματα στα Πληροφοριακά Συστήματα (π.χ. μη εξουσιοδοτημένη δραστηριότητα, κλοπή μηχανογραφικού εξοπλισμού, απάτη, παραβίαση ασφάλειας, μη διαθεσιμότητα συστημάτων, καταστροφή μηχανογραφικού εξοπλισμού, κακόβουλη χρήση, κα) και ενημέρωσης των αρμόδιων υπηρεσιακών μονάδων (Διαχείρισης Κινδύνων και Εσωτερικής Επιθεώρησης), για την αποτελεσματικότερη καταγραφή και αντιμετώπιση του λειτουργικού κινδύνου. Η καταγραφή θα πρέπει να είναι συστηματική με στόχο την δημιουργία ιστορικότητας και λεπτομερής έτσι ώστε να περιγράφει με σαφήνεια το γεγονός. Οι σχετικές πληροφορίες θα πρέπει να καταγράφονται ηλεκτρονικά και να δομούνται με τέτοιο τρόπο ώστε να διευκολύνεται η αυτόματη παραγωγή αναφορών αλλά και η άμεση ενημέρωση των εμπλεκόμενων υπηρεσιακών μονάδων.

12. να διαθέτει Σύστημα Διοικητικής Πληροφόρησης (M.I.S. - Management Information System), κατάλληλο για την αποτελεσματική πληροφόρηση της Διοίκησης του ΠΙ. Ένα τέτοιο σύστημα θα πρέπει να χαρακτηρίζεται από την ομοιόμορφη και βάσει καταγεγραμμένων διαδικασιών συλλογή και επεξεργασία, την έγκαιρη διάθεση, την ακρίβεια, την αξιοπιστία, και την πληρότητα των πληροφοριών. Η συλλογή και επεξεργασία των απαραίτητων πληροφοριών θα πρέπει να γίνεται όσο το δυνατόν πιο αυτοματοποιημένα.

13. να γνωρίζει και να συμμορφώνεται με το νομικό, εποπτικό και κανονιστικό πλαίσιο σε ό,τι αφορά θέματα πληροφορικής.

14. να μελετά, να αξιολογεί και να εφαρμόζει, όπου κρίνει απαραίτητο, τα διεθνή πρότυπα και μεθοδολογίες διαχείρισης και ασφάλειας των Πληροφοριακών Συστημάτων, καθώς επίσης να παρακολουθεί και να λαμβάνει υπόψη τις διεθνείς εξελίξεις στους συγκεκριμένους τομείς.

Α2. Οργάνωση Υπηρεσιακής Μονάδας Πληροφορικής

Το Πιστωτικό Ίδρυμα θα πρέπει να διαθέτει εξειδικευμένη Υπηρεσιακή Μονάδα Πληροφορικής, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, η οποία θα πρέπει:

1. να διαθέτει οργανόγραμμα στο οποίο:

- απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της μονάδας και περιγράφονται με σαφήνεια οι αρμοδιότητες των επί μέρους υπηρεσιακών μονάδων που το αποτελούν,
- απεικονίζεται ο διαχωρισμός των καθηκόντων προκειμένου να αποκλείεται η ύπαρξη ασυμβίβαστων ρόλων, παρέχεται η δυνατότητα καταλογισμού των ευθυνών και αξιοποιούνται με τον καταλληλότερο τρόπο οι δυνατότητες του προσωπικού. Ειδικότερα, θα πρέπει να διασφαλίζεται ότι διαχωρίζονται πλήρως οι λειτουργίες που σχετίζονται με το σχεδιασμό και την ανάπτυξη των συστημάτων από τις λειτουργίες που αφορούν στην καθημερινή λειτουργία τους,
- προβλέπεται, ανάλογα με το μέγεθος του ΠΙ και την πολυπλοκότητα των συστημάτων, υπηρεσιακή Μονάδα Ασφάλειας των ΠΣ. Η συγκεκριμένη υπηρεσιακή μονάδα, μαζί με τον Υπεύθυνο Ασφάλειας των ΠΣ, πρέπει να διαμορφώνουν ολοκληρωμένη εικόνα για το επίπεδο ασφάλειας των συστημάτων και τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους. Στις αρμοδιότητές τους περιλαμβάνονται, μεταξύ άλλων, η συμμετοχή στην αξιολόγηση και διαχείριση των κινδύνων των ΠΣ, η σύνταξη και ενημέρωση της πολιτικής ασφάλειας, η συμμετοχή στη διαδικασία εύρεσης λύσεων για την κάλυψη κενών ασφάλειας και την αντιμετώπιση έκτακτων περιστατικών κα.
- εξασφαλίζεται η αναπλήρωση του προσωπικού τουλάχιστον στις κρίσιμες μηχανογραφικές λειτουργίες.

2. να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες περιγραφές θέσεων εργασίας στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση.

Α3. Σχέσεις με Εξωτερικούς Συνεργάτες

Όταν το ΠΙ συνεργάζεται με εξωτερικούς συνεργάτες σε θέματα πληροφορικής (Πάροχοι Υπηρεσιών Πληροφορικής - Π.Υ.Π., προμηθευτές, κ.λπ.) κατά τα προβλεπόμενα στο Παράρτημα 1 της παρούσας Πράξης, θα πρέπει να λαμβάνονται υπόψη ειδικότερα τα εξής:

1. η χρήση εξωτερικών συνεργατών, ενώ μπορεί να επιλύει σημαντικά προβλήματα, δημιουργεί πεδίο πρόσθετων κινδύνων για το ΠΙ, οι οποίοι πρέπει να εντοπισθούν, εκτιμηθούν και αντιμετωπισθούν αποτελεσματικά. Στους κινδύνους αυτούς περιλαμβάνονται:

- η έλλειψη ουσιαστικού ελέγχου στις προσφερόμενες υπηρεσίες,
- η εξάρτηση από τρίτους,
- η απώλεια εσωτερικής τεχνογνωσίας,

● η ενδεχόμενη αδυναμία άμεσης προσαρμογής στις απαιτήσεις των πελατών και του οικονομικού περιβάλλοντος,

● η αδιαφανής κοστολόγηση των προσφερόμενων υπηρεσιών,

● η διαφορά νοοτροπίας μεταξύ ΠΙ και παρόχου, κ.λπ.

2. σε περίπτωση που αποφασίσει να αναθέσει μέρος ή και το σύνολο των υπηρεσιών πληροφορικής σε εξωτερικούς συνεργάτες, πρέπει να τηρούνται οι αρχές του Παραρτήματος 1 της παρούσας Πράξης για:

● την αξιολόγηση των κινδύνων που απορρέουν από μια πιθανή συνεργασία,

● τον τρόπο επιλογής των εξωτερικών συνεργατών,

● την επάρκεια των προς υπογραφή συμβολαίων,

● την εποπτεία και τον έλεγχο της επαρκούς και ασφαλούς λειτουργίας των συστημάτων.

3. η ανάθεση υλοποίησης σημαντικών για το ΠΙ συστημάτων σε τρίτους, θα πρέπει να αιτιολογείται από την Ειδική Συντονιστική Επιτροπή Πληροφορικής εγγράφως προς τη Διοίκηση, η οποία και παρέχει την τελική έγκρισή της.

4. κατά το στάδιο της επιλογής του εξωτερικού συνεργάτη, πέραν της αξιολόγησης των προσφερομένων υπηρεσιών θα πρέπει να αξιολογούνται, με βάση το μέγεθος και την κρισιμότητα της συνεργασίας:

● η οικονομική κατάσταση και η μακροπρόθεσμη βιωσιμότητά του,

● η επίδραση του προς υπογραφή συμβολαίου στον κύκλο εργασιών του,

● η φήμη του στην αγορά, το πελατολόγιο και ο βαθμός ικανοποίησης των πελατών του,

● η οργανωτική του δομή (για την παροχή και αποτελεσματική υποστήριξη των υπηρεσιών),

● η αριθμητική και ποιοτική επάρκεια του στελεχικού δυναμικού,

● η ασφαλιστική του κάλυψη, κλπ.

Στις περιπτώσεις που ο εξωτερικός συνεργάτης κάνει χρήση συνεργιών για την υλοποίηση των έργων θα πρέπει να αξιολογηθούν ανάλογα και οι συνέργιες αυτές.

5. από τεχνικής άποψης θα πρέπει να αξιολογούνται:

● η ποιότητα και επάρκεια της υπάρχουσας Πολιτικής Ασφάλειας του παρόχου,

● η αξιοπιστία των συστημάτων,

● η καταλληλότητα της τεχνολογίας που χρησιμοποιείται,

● η πληρότητα των διαδικασιών υποστήριξης των παρεχομένων υπηρεσιών,

● τα σχέδια συνέχειας εργασιών και ανάκαμψης από καταστροφή του παρόχου.

Πορίσματα εσωτερικών και εξωτερικών ελεγκτών για τον εξωτερικό συνεργάτη - εάν είναι διαθέσιμα - αποτελούν πολύτιμες πηγές πληροφόρησης για τη διαμόρφωση πληρέστερης εικόνας.

6. στο προς υπογραφή συμβόλαιο θα πρέπει - μεταξύ άλλων - να περιγράφονται αναλυτικά και με σαφήνεια:

● τα δικαιώματα και οι υποχρεώσεις των συμβαλλομένων μερών,

● το συμφωνηθέν επίπεδο παροχής υπηρεσιών (Service Level Agreement - SLA) και ο τρόπος τιμολόγησής τους,

● η δυνατότητα επαναδιαπραγμάτευσης του συμβολαίου,

● τα θέματα ιδιοκτησίας (ownership), αδειοδότησης (licensing) και πνευματικών δικαιωμάτων,

● οι περιπτώσεις υπεργολαβίας (sub-contracting),

● οι διαδικασίες επίλυσης διαφορών,

● οι διαδικασίες τερματισμού του συμβολαίου (π.χ. οι διαδικασίες παράδοσης του πηγαίου κώδικα και των δεδομένων τους - Escrow Agreement).

Ειδική αναφορά θα πρέπει επίσης να γίνεται:

● στην ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα και δυνατότητα ανίχνευσης) των πληροφοριών,

● στην πιστοποίηση των συναλλασσομένων μερών και στη μη αποποίηση των συναλλαγών,

● στην ασφάλεια των διασυνδέσεων μεταξύ του ΠΙ και του εξωτερικού συνεργάτη,

● στις ποινικές ρήτρες για τις περιπτώσεις παραβίασης των συμφωνηθέντων,

● στη δυνατότητα διενέργειας ελέγχων εκ μέρους του ΠΙ (Right to Audit),

● στη δυνατότητα διενέργειας ελέγχων από τρίτους για λογαριασμό του ΠΙ,

● στο είδος και τη συχνότητα των αναφορών ή αρχείων που θα ανταλλάσσουν τα δύο μέρη,

● στα σχέδια συνέχειας εργασιών και ανάκαμψης από καταστροφή του εξωτερικού συνεργάτη.

Β. ΑΝΑΠΤΥΞΗ ΚΑΙ ΠΡΟΜΗΘΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Ο κύκλος ζωής ενός συστήματος πρέπει να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, συνήθως, είναι η φάση της Μελέτης Σκοπιμότητας, της Ανάλυσης των Επιχειρησιακών Απαιτήσεων και του Καθορισμού των Προδιαγραφών, της Τεχνικής Ανάλυσης και του Σχεδιασμού, της Ανάπτυξης, των Δοκιμών, της Αποδοχής και της Μεταφοράς στην Παραγωγή, της Λειτουργίας και Υποστήριξης και τέλος της Απόσυρσης. Η μετάβαση από τη μία φάση στην άλλη προϋποθέτει την ανασκόπηση και έγκριση των αποτελεσμάτων της προηγούμενης.

Η εποπτεία του έργου της ανάπτυξης κάθε σημαντικού συστήματος πρέπει να ανατίθεται στη Συντονιστική Επιτροπή της Πληροφορικής (IT Steering Committee). Με την ολοκλήρωση της ανάπτυξης του συστήματος, η επιχειρησιακή και τεχνική του εποπτεία θα πρέπει να ανατίθεται στις αρμόδιες υπηρεσιακές μονάδες ή στελέχη.

Πριν την ανάπτυξη ή προμήθεια ενός σημαντικού συστήματος πρέπει να γίνεται Μελέτη Σκοπιμότητας. Στη φάση αυτή θα πρέπει, μεταξύ άλλων, να ορίζονται οι λειτουργίες που θα καλύπτονται από το νέο σύστημα, να εκτιμάται η σχέση κόστους / οφέλους (μείωση στα τρέχοντα κόστη, αύξηση απόδοσης, βελτίωση της εικόνας του ΠΙ) που θα επιφέρει το νέο σύστημα και να εξετάζεται η δυνατότητα υλοποίησης του συστήματος τόσο από την πλευρά του ανθρώπινου δυναμικού όσο και από αυτή του μηχανογραφικού εξοπλισμού / λογισμικού. Τέλος, θα πρέπει να εκτιμάται το κόστος ανάπτυξης, λειτουργίας, και υποστήριξης του συστήματος και να συγκρίνεται το κόστος εσωτερικής ανάπτυξης με αυτό της προμήθειας ή της ανάθεσης σε τρίτους.

Β1. Ανάπτυξη Συστημάτων

Στις περιπτώσεις που το ΠΙ επιλέγει την εσωτερική ανάπτυξη ενός Πληροφοριακού Συστήματος, θα πρέπει:

1. πριν την έναρξη της ανάπτυξης, να ορισθεί Ομάδα Έργου που θα αναλάβει την διαχείριση του έργου και την κατάρτιση ενός χρονοδιαγράμματος υλοποίησης. Η Ομάδα Έργου ανάλογα με την κρισιμότητα και το μέγεθος του συστήματος θα πρέπει να απαρτίζεται από τον επικεφαλής της, τον υπεύθυνο για την ασφάλεια του συστήματος, αναλυτές / προγραμματιστές και εκπροσώπους χρηστών ή άλλων εμπλεκόμενων μερών.

2. το χρονοδιάγραμμα υλοποίησης να προσδιορίζει, μεταξύ άλλων, τις φάσεις, τη διάρκεια τους, και τους υπεύθυνους για την υλοποίηση της κάθε φάσης, καθώς και τα παραδοτέα. Επιπλέον, στο χρονοδιάγραμμα θα πρέπει να προβλέπεται ο ακριβής χρόνος παράδοσης μηχανογραφικού εξοπλισμού και άλλων υπηρεσιών από προμηθευτές εφόσον επηρεάζει τον χρονοπρογραμματισμό του έργου.

3. να ορίζεται ένα σχέδιο επικοινωνίας, στο οποίο θα καθορίζονται οι διαδικασίες ενημέρωσης των εμπλεκομένων μερών για την πρόοδο του έργου, επικοινωνίας των θεμάτων προς επίλυση προς τα ανώτερα στελέχη, επικοινωνίας του Πιστωτικού Ιδρύματος με προμηθευτές και κοινοποίησης των αλλαγών που θα επιφέρει το νέο σύστημα στον οργανισμό.

4. να λαμβάνονται υπόψη θέματα αποδοχής και αποτελεσματικής λειτουργίας του νέου πληροφοριακού συστήματος από το προσωπικό του Πιστωτικού Ιδρύματος και να υιοθετείται σχέδιο διαχείρισης των λειτουργικών αλλαγών ώστε να αντιμετωπιστούν φαινόμενα μη αποτελεσματικής εξυπηρέτησης των πελατών λόγω έλλειψης εξοικείωσης με το νέο πληροφοριακό σύστημα.

5. οι πληροφορίες που συλλέγονται κατά τη διάρκεια της φάσης της Ανάλυσης των Επιχειρησιακών Απαιτήσεων και του Καθορισμού των Προδιαγραφών να αφορούν τα προβλήματα, τις απαιτήσεις και τις ανάγκες βελτίωσης που έχουν εντοπίσει οι χρήστες σχετικά με το σύστημα. Οι απαιτήσεις θα πρέπει να καθορίζουν το τι πρέπει να κάνει το σύστημα και όχι το πώς, ενώ οι προδιαγραφές θα πρέπει να προσδιορίζουν σε γενικές γραμμές το πώς θα μπορέσουν να υλοποιηθούν οι απαιτήσεις των χρηστών. Κατά τη φάση του καθορισμού των προδιαγραφών του νέου συστήματος θα πρέπει να εξεταστεί κατά πόσο αυτό θα πρέπει να συνεργάζεται και σε ποιο επίπεδο με τα υπάρχοντα συστήματα του ΠΙ.

6. να γίνεται εκτίμηση του όγκου των δεδομένων και του αριθμού των συναλλαγών που θα διαχειρίζεται το νέο σύστημα, λαμβάνοντας υπόψη τις τρέχουσες αλλά και τις μελλοντικές ανάγκες έτσι ώστε να προσδιοριστούν με μεγαλύτερη ακρίβεια οι προδιαγραφές του μηχανογραφικού εξοπλισμού του συστήματος.

7. να γίνει λεπτομερής σχεδιασμός για τη διαχείριση των δεδομένων του προϋπάρχοντος μηχανογραφικού ή μη συστήματος και να περιλαμβάνει θέματα εκκαθάρισης παλαιών δεδομένων (data cleansing), μετατροπής δεδομένων στην μορφή του νέου συστήματος (data conversion) και μετάπτωσης δεδομένων (data migration).

8. στις φάσεις της Τεχνικής Ανάλυσης και του Σχεδιασμού να διενεργείται Ανάλυση Κινδύνων και να καθορίζονται με λεπτομέρεια οι απαιτήσεις ασφαλούς λειτουργίας του συστήματος σύμφωνα και με όσα προβλέπει η ισχύουσα Πολιτική Ασφάλειας του ΠΙ, οι τεχνικές προδιαγραφές του (οι οποίες περιλαμβάνουν, μεταξύ άλλων, τον καθορισμό των παραμέτρων της λογικής ασφάλειας του συστήματος), ο έλεγχος και η συμφωνία των δεδομένων και η δομή των απαραίτητων αρχείων καταγραφής (audit trails και logs) για τα οποία θα πρέπει να λαμβάνονται υπόψη οι σχετικές συστάσεις της Ευρωπαϊκής Επιτροπής για τα Τραπεζικά Πρότυπα ("The Use of Audit Trails in Security Systems: Guidelines for European Banks").

Στις συγκεκριμένες φάσεις είναι αναγκαία η συνεργασία με τη Μονάδα Εσωτερικής Επιθεώρησης για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, καθώς και των ελεγκτικών αρχείων καταγραφής και αναφορών που θα παράγονται για τη διευκόλυνση του ελέγχου. Η συνεργασία αυτή δεν επηρεάζει το ελεγκτικό έργο της Μονάδας Εσωτερικής Επιθεώρησης για το εν λόγω σύστημα.

9. η Ανάπτυξη του Συστήματος να υλοποιείται σε ξεχωριστό μηχανογραφικό περιβάλλον από αυτό της παραγωγής και να ακολουθεί πρότυπα που έχουν τεθεί από το ΠΙ (π.χ. χρήση συγκεκριμένων εργαλείων και μεθοδολογίας ανάπτυξης προγραμμάτων) με στόχο την ομοιογένεια των Πληροφοριακών Συστημάτων και την ευκολία υποστήριξής τους.

10. οι Δοκιμές του Συστήματος να διενεργούνται σε πρώτη φάση από το προσωπικό της Πληροφορικής σε ξεχωριστό περιβάλλον με προκαθορισμένα σενάρια. Σε δεύτερη φάση θα πρέπει να γίνονται τεκμηριωμένες και ολοκληρωμένες δοκιμές που περιλαμβάνουν:

- δοκιμές επαναφοράς (recovery testing) ελέγχοντας την δυνατότητα επαναφοράς του συστήματος σε περιπτώσεις βλάβης του λογισμικού ή του μηχανογραφικού εξοπλισμού,
- δοκιμές ασφαλείας (security testing) ελέγχοντας ότι το σύστημα περιλαμβάνει τις δικλείδες ασφαλείας, όπως αυτές προδιαγράφηκαν κατά τον σχεδιασμό του συστήματος,
- δοκιμή αντοχής (stress test) του συστήματος σε συνθήκες επεξεργασίας αυξημένου όγκου δεδομένων.

Στις δοκιμές αυτές είναι απαραίτητο να συμμετέχουν, πέραν των προγραμματιστών, η Μονάδα Διασφάλισης Ποιότητας (όπου υπάρχει), ο Υπεύθυνος Ασφάλειας (Security Officer) και η Μονάδα Εσωτερικής Επιθεώρησης.

11. για την Αποδοχή του Συστήματος να διενεργούνται ολοκληρωμένες δοκιμές με όσο το δυνατόν πιο πιστή προσομοίωση των συνθηκών παραγωγής. Στην περίπτωση που νέο σύστημα αντικαθιστά παλαιότερο θα πρέπει τα δύο συστήματα για ένα χρονικό διάστημα να λειτουργήσουν παράλληλα με τα ίδια δεδομένα (parallel run) και να γίνεται σύγκριση των αποτελεσμάτων τους. Οι συμμετέχοντες θα πρέπει να αποφασίζουν για την αποδοχή ή μη του συστήματος και γνωστοποιούν εγγράφως την απόφασή τους.

12. η Μεταφορά του νέου Συστήματος στην παραγωγή να πραγματοποιείται από εξειδικευμένο προσωπικό (π.χ. librarians) βάσει καταγεγραμμένων οδηγιών, σε χρονική περίοδο που δεν εκτελούνται άλλες σημαντικές εργασίες και με την πρόβλεψη για τη δυνατότητα - σε περίπτωση προβλήματος - επαναφοράς στην αρχική κατάσταση.

13. το σύστημα, πριν ακόμη τεθεί σε λειτουργία, να διαθέτει πλήρη τεκμηρίωση που θα ακολουθεί συγκεκριμένα ποιοτικά πρότυπα που έχουν τεθεί από το ίδιο το

ΠΙ. Τα εγχειρίδια της τεκμηρίωσης θα πρέπει να έχουν ενιαία μορφή και δομή.

14. να πραγματοποιείται εκπαίδευση των χρηστών του συστήματος σε ξεχωριστό μηχανογραφικό περιβάλλον, το οποίο και δεν θα επηρεάζεται από τα μηχανογραφικά περιβάλλοντα ανάπτυξης και παραγωγής. Τα συγκεκριμένα περιβάλλοντα συνιστάται να παραμένουν ενεργά έτσι ώστε να χρησιμοποιούνται στις περιπτώσεις που το σύστημα υφίσταται αλλαγές.

15. η Λειτουργία και Υποστήριξη του Συστήματος να περιλαμβάνει διαδικασίες ελέγχου των αλλαγών (change control), ελέγχου των εκδόσεων του συστήματος (versioning), ελέγχου ενημερώσεων του συστήματος για την αντιμετώπιση προβλημάτων που εντοπίστηκαν (patching), ελέγχου της απόδοσης του συστήματος, λήψης και φύλαξης εφεδρικών αρχείων, συνέχειας των εργασιών, ενημέρωσης του Help Desk για την υποστήριξη των χρηστών του συστήματος, κα.

16. η φάση Απόσυρσης του Συστήματος να περιλαμβάνει διαδικασίες για τη διατήρηση των πληροφοριών σύμφωνα με τις νομικές και εποπτικές οδηγίες (information preservation), τη διαγραφή των πληροφοριών από τα μέσα αποθήκευσης (media sanitization), την απόσυρση του υλικού και λογισμικού (hardware & software disposal). Στη συγκεκριμένη φάση πρέπει να διασφαλίζεται η αποτελεσματική συνέχεια της λειτουργίας των συστημάτων που διασυνδέονται με το σύστημα που αποσύρεται.

Β2. Προμήθεια Συστημάτων

Στις περιπτώσεις που το ΠΙ αποφασίζει την προμήθεια Πληροφοριακών Συστημάτων, θα πρέπει, εκτός των προαναφερθέντων:

1. η όλη διαδικασία προμήθειας να χαρακτηρίζεται από διακριτές φάσεις, οι οποίες θα υλοποιούν πρότυπα, μεθοδολογίες και διαδικασίες επίσημα καταγεγραμμένες και εγκεκριμένες. Τέτοιες φάσεις, είναι αυτές της πρόσκλησης για υποβολή προτάσεων (Request For Proposal - RFP) με αναλυτική περιγραφή των αναγκών που θα καλύπτει το προς προμήθεια σύστημα, της επιλογής του εξωτερικού συνεργάτη, της σύναψης της συμφωνίας και της υπογραφής του συμβολαίου, της ένταξης και λειτουργίας των συστημάτων στην παραγωγή και, τέλος, της εποπτείας και του ελέγχου τους.

2. η επιλογή του συστήματος να γίνεται με βάση τις αναλυτικές προδιαγραφές που οφείλει να θέτει το ΠΙ, τις δυνατότητες επέκτασης και προσαρμογής του στις διαρκώς αυξανόμενες επιχειρησιακές ανάγκες, τη φιλικότητα προς τον χρήστη, τις δυνατότητες ασφαλούς λειτουργίας (λογική ασφάλεια, audit trails & logs), το επίπεδο υποστήριξης, το σύστημα αναφορών του κλπ.

3. το είδος παρέμβασης του ΠΙ στο σύστημα να είναι εκ των προτέρων αυστηρά καθορισμένο. Οι όποιες παρεμβάσεις θα πρέπει να ακολουθούν εγκεκριμένες και καταγεγραμμένες διαδικασίες, να υλοποιούνται από εξειδικευμένο προσωπικό και να διατηρούνται στο ελάχιστο δυνατό επίπεδο έτσι ώστε να μην αλλοιώνεται η φυσιογνωμία του συστήματος και να είναι εύκολη η αναβάθμιση και συντήρησή του. Σημειώνεται ότι, σε περίπτωση σημαντικής απόκλισης των λειτουργικών διαδικασιών του ΠΙ από εκείνες που υποστηρίζει το αγορασθέν σύστημα, το ΠΙ είναι αυτό που συνήθως θα πρέπει να προσαρμόσει τις λειτουργικές του διαδικασίες στα χαρακτηριστικά του συστήματος και όχι το αντίστροφο.

4. στα κεντρικά συστήματα τραπεζικών εργασιών, η ανάπτυξη περιφερειακών εφαρμογών που θα αντλούν πληροφορίες από το κεντρικό σύστημα και θα υλοποιούν τοπικές αλλά και επιχειρησιακές ιδιαιτερότητες να γίνεται με βάση τα ισχύοντα στο ΠΙ πρότυπα για την ανάπτυξη εφαρμογών, έτσι ώστε να διατηρείται η μηχανογραφική ομοιογένεια.

5. ο τρόπος υποστήριξης των συστημάτων να είναι αυστηρά προδιαγεγραμμένος, με σαφή καθορισμό των περιπτώσεων στις οποίες απαιτείται υποστήριξη από τον πάροχο αλλά και των χρονικών περιθωρίων ανταπόκρισής του.

6. οι περιπτώσεις απομεμακρυσμένης πρόσβασης του παρόχου στα συστήματα του ΠΙ για την επίλυση εκτάκτων προβλημάτων, να είναι εξαιρετικά περιορισμένες, να αντιμετωπίζονται με ιδιαίτερη προσοχή, και σε κάθε περίπτωση να υπάρχει πλήρης καταγραφή (logging) των ενεργειών του.

7. να είναι απαραίτητη η απόκτηση τεχνογνωσίας, όχι μόνον μέσω της κατάλληλης εκπαίδευσης του εμπλεκόμενου στη λειτουργία τέτοιων συστημάτων προσωπικού, αλλά κυρίως μέσω της συμμετοχής του σε όλες τις φάσεις εξέλιξης των συστημάτων, έτσι ώστε η εξάρτηση του ΠΙ από τον προμηθευτή βαθμιαία να ελαττώνεται.

8. εφόσον έχουν υλοποιηθεί οι απαιτήσεις του ΠΙ - όπως αυτές αναφέρονται στο συμβόλαιο - και μετά το πέρας των απαραίτητων δοκιμών εκ μέρους του παρόχου, να υφίσταται διαδικασία επίσημης αποδοχής και παραλαβής του συστήματος εκ μέρους του ΠΙ με τη συμμετοχή όλων των εμπλεκομένων μερών.

Γ. ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ

Η απρόσκοπτη λειτουργία των Πληροφοριακών Συστημάτων και η αποτελεσματική υποστήριξή τους είναι παράγοντες κρίσιμοι τόσο για την εύρυθμη λειτουργία του ΠΙ και τη δημιουργία σχέσεων εμπιστοσύνης με τους πελάτες, όσο και για την αποτελεσματική αντιμετώπιση του λειτουργικού κινδύνου. Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη των Πληροφοριακών Συστημάτων προϋποθέτουν την τήρηση των πολιτικών, προτύπων και διαδικασιών του ΠΙ από όλες τις εμπλεκόμενες υπηρεσιακές μονάδες, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

Γ1. Λειτουργία Συστημάτων

Ο όρος «Λειτουργία Συστημάτων» αναφέρεται στο σύνολο των διαδικασιών που απαιτούνται για την καθημερινή λειτουργία των Πληροφοριακών Συστημάτων σε ένα Πιστωτικό Ίδρυμα. Για ένα αποδεκτό επίπεδο ασφαλούς και αποτελεσματικής λειτουργίας τους θα πρέπει να υφίστανται:

1. πλήρης και λεπτομερής καταγραφή του μηχανογραφικού εξοπλισμού (κεντρικά συστήματα, εξυπηρετητές, προσωπικοί υπολογιστές, περιφερειακά, δίκτυα και τηλεπικοινωνίες), του αρχιτεκτονικού σχεδιασμού, του χρησιμοποιούμενου λογισμικού, καθώς και του ιστορικού των εκδόσεων, των ενημερώσεων, και των αδειών χρήσης. Αρχείο πρέπει να τηρείται επίσης για τα μέσα που αποθηκεύουν και διακινούν ευαίσθητα δεδομένα του οργανισμού (cartridges, ταινίες, δισκέτες, CDs, εκτυπώσεις, microfiche κα). Τα αρχεία καταγραφής θα πρέπει να ενημερώνονται άμεσα στις περιπτώσεις αλλαγών.

2. τήρηση πλήρους και ενημερωμένης τεκμηρίωσης για κάθε σύστημα με τα επίσημα εγχειρίδια των εται-

ρειών που προμηθεύουν το υλικό και το λογισμικό των συστημάτων, και τα εγχειρίδια που συντάσσονται από το προσωπικό του ΠΙ.

3. επαρκής συντήρηση και τεχνική υποστήριξη των συστημάτων με βάση πάντοτε τις προδιαγραφές τους και τις ανάγκες που προκύπτουν.

4. υποστήριξη των υπαλλήλων-χρηστών εντός, αλλά και των πελατών-χρηστών εκτός του οργανισμού (π.χ. ηλεκτρονική τραπεζική), η οποία και θα πρέπει να ανατίθεται σε κατάλληλα οργανωμένες και στελεχωμένες υπηρεσιακές μονάδες (Help Desk). Στην υποστήριξη θα πρέπει να λαμβάνεται υπόψη το είδος του χρήστη και η φύση του προβλήματος που αντιμετωπίζει. Το πλήθος και το είδος των προβλημάτων θα πρέπει να καταγράφονται και να τυγχάνουν στατιστικής επεξεργασίας.

5. διαδικασίες διαχείρισης των παραμέτρων λειτουργίας των συστημάτων.

6. διαδικασίες αποτροπής εγκατάστασης και χρήσης μη εγκεκριμένου από το ΠΙ λογισμικού, καθώς επίσης λογισμικού χωρίς την κατάλληλη αδειοδότηση.

7. προγραμματισμός των εργασιών προς εκτέλεση, καταγραφή των προβλημάτων που προκύπτουν και των ενεργειών που πρέπει να γίνονται στις έκτακτες περιπτώσεις, κλπ. Η επιτυχής ή μη εκτέλεση των προγραμματισμένων αλλά και έκτακτων εργασιών θα πρέπει να καταχωρείται σε ειδικό ημερολόγιο, το οποίο και θα φέρει τις υπογραφές του προσωπικού που τις εκτέλεσε. Η εκτέλεση έκτακτων εργασιών θα πρέπει να γίνεται κατόπιν ειδικής έγκρισης.

8. έλεγχος των δεδομένων, για εξασφάλιση της ακεραιότητας, ορθότητας και εμπιστευτικότητάς τους, σε όλες τις φάσεις επεξεργασίας τους. Οι κάθε είδους ασυμφωνίες θα πρέπει να διαπιστώνονται και να αντιμετωπίζονται βάσει καταγεγραμμένων διαδικασιών.

9. διαδικασίες διαχείρισης της χωρητικότητας, του φόρτου και της απόδοσης των συστημάτων και δικτύων.

10. συνεχής παρακολούθηση της διαθεσιμότητας των συστημάτων και των δικτύων. Ειδικότερα για τα κρίσιμα συστήματα, το ΠΙ πρέπει να είναι σε θέση να υπολογίζει το ποσοστό διαθεσιμότητάς τους σε επίπεδο έτους και να το συγκρίνει με προκαθορισμένους στόχους. Επιπλέον, το ΠΙ θα πρέπει να διαθέτει διαδικασίες λεπτομερούς καταγραφής των συμβάντων μη διαθεσιμότητας (επηρεαζόμενα συστήματα, χρονική διάρκεια μη διαθεσιμότητας, αιτία προβλήματος, τρόπος και χρονική διάρκεια αντιμετώπισης, συχνότητα εμφάνισης, κόστος για το ΠΙ) και άμεσης ενημέρωσης των αρμόδιων λειτουργικών μονάδων (Εσωτερικής Επιθεώρησης, Διαχείρισης Κινδύνων) και της Διοίκησης.

11. επαρκείς διαδικασίες διαχείρισης αντιγράφων ασφαλείας (λεπτομερής αναφορά στο κεφάλαιο Γ4).

12. ειδικότερα, για τα συστήματα και τις υπηρεσίες Ηλεκτρονικής Τραπεζικής θα πρέπει να υφίστανται:

i. επαρκής πληροφόρηση στο διαδικτυακό τόπο (web site) του ΠΙ, έτσι ώστε να μπορούν οι εν δυνάμει πελάτες τους να έχουν μια επαρκή γνώση για την ταυτότητα του ΠΙ και την εποπτεύουσα αρχή που παρέχει την άδεια λειτουργίας, πριν πραγματοποιήσουν τις ηλεκτρονικές τους συναλλαγές. Επίσης, γνωστοποίηση του τρόπου με τον οποίο μπορούν να επικοινωνήσουν οι πελάτες με το σχετικό κέντρο υποστήριξης σε περίπτωση πάσης φύσεως προβλήματος, το ψηφιακό πιστοποιητικό του διαδικτυακού τόπου, το οποίο θα πρέπει να έχει εκδοθεί από επίσημη αρχή πιστοποίησης, πληροφορίες για την ασφαλή χρήση των παρεχομένων υπηρεσιών κ.λπ.

ii. ενημέρωση των πελατών για την πολιτική εμπιστευτικότητας που εφαρμόζει το ΠΙ σε σχέση με τα προσωπικά τους δεδομένα. Η πληροφόρηση αυτή συνιστάται να παρέχεται και μέσα από το διαδικτυακό τόπο του ιδρύματος. Παροχή επίσης στους πελάτες του δικαιώματος να αρνηθούν την διάθεση - εκχώρηση σε τρίτους δεδομένων που τους αφορούν, για προώθηση προϊόντων ή άλλο λόγο. Τα δεδομένα των πελατών θα πρέπει να χρησιμοποιούνται μόνον για τους σκοπούς για τους οποίους οι πελάτες γνωρίζουν ότι τα διαθέτουν.

iii. σαφής σήμανση στο διαδικτυακό τόπο του ΠΙ των συνδέσεων (links) με διαδικτυακούς τόπους άλλων εταιρειών ή οργανισμών. Πρέπει να φαίνεται έκδηλα στον πελάτη ότι, όταν εγκαταλείπει το διαδικτυακό τόπο του ΠΙ, συνδέεται με μια εντελώς ξεχωριστή επιχειρηματική μονάδα ή άλλη νομική οντότητα.

iv. αυτοματοποιημένα συστήματα παρακολούθησης των συναλλαγών, τα οποία και θα βασίζουν την αποτελεσματική λειτουργία τους στη δημιουργία εκ μέρους του ΠΙ στατιστικών προτύπων κίνησης λογαριασμού για κάθε πελάτη. Τα συστήματα αυτά, με βάση τα διαμορφωμένα χαρακτηριστικά κίνησης των λογαριασμών των πελατών (profiles), θα πρέπει να εντοπίζουν και να καταγράφουν ασυνήθιστες συναλλακτικές συμπεριφορές και να παράγουν, σε πραγματικό χρόνο, προειδοποιητικά μηνύματα (alerts) για τη διερεύνηση ενδεχόμενων περιπτώσεων απάτης.

v. αποτελεσματική αντιμετώπιση των κινδύνων νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες (money laundering) και χρηματοδότησης της τρομοκρατίας. Οι συγκεκριμένοι κίνδυνοι στην ηλεκτρονική τραπεζική είναι ιδιαίτερα αυξημένοι λόγω της ευκολίας χρήσης των υπηρεσιών από οπουδήποτε και οποιαδήποτε χρονική στιγμή, της απρόσωπης φύσης των συναλλαγών και της αυτόματης διεκπεραίωσής τους. Ως εκ τούτου, το ΠΙ θα πρέπει να μεριμνά για την εγκατάσταση αυτοματοποιημένων συστημάτων και εργαλείων διαχείρισης των συναλλαγών, τα οποία κατ' ελάχιστον θα θέτουν όρια σε συγκεκριμένες ομάδες ή κατηγορίες συναλλαγών, θα παρέχουν τη δυνατότητα καθυστέρησης εκτέλεσης της συναλλαγής μέχρι την εξακρίβωση συγκεκριμένων στοιχείων (filters & monitoring tools/systems) κ.λπ.

vi. δυνατότητα εύκολης προσπέλασης και επεξεργασίας στοιχείων παλαιότερων συναλλαγών, έτσι ώστε να γίνεται εφικτός ο εντοπισμός συναλλακτικών ιδιαιτεροτήτων και ανωμαλιών, για να διευκολύνεται η στοιχειοθέτηση αποδεικτικών στοιχείων και η επαρκής πληροφόρηση των εποπτικών αρχών, ειδικά στις περιπτώσεις απάτης και νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και χρηματοδότησης της τρομοκρατίας, παροχής επενδυτικών υπηρεσιών κλπ.

vii. εγχειρίδια σε ηλεκτρονική ή έντυπη μορφή, τα οποία θα ενημερώνουν τους πελάτες για τον τρόπο χρήσης των συστημάτων με έμφαση σε θέματα ασφάλειας. Επιπλέον, το ΠΙ θα πρέπει να εφοδιάζει τους χρήστες με πρακτικές ασφαλούς χρήσης των προσωπικών υπολογιστών μέσω των οποίων προσπελαύνονται ορισμένα συστήματα ηλεκτρονικής τραπεζικής και ηλεκτρονικών πληρωμών. Στις πρακτικές αυτές θα πρέπει να γίνεται αναφορά, μεταξύ άλλων, σε θέματα προστασίας από ιούς και άλλο κακόβουλο λογισμικό, ασφαλούς απο-

θήκευσης και χρήσης προσωπικών κωδικών (ειδικά σε υπολογιστές κοινής χρήσης οι οποίοι γενικά θα πρέπει να αποφεύγονται για τέτοια χρήση).

viii. επαρκείς διαδικασίες ασφάλειας με έμφαση στη πιστοποίηση των συναλλασσομένων μερών (ψηφιακό πιστοποιητικό διαδικτυακού τόπου ΠΙ, πιστοποίηση δύο επιπέδων για τον πελάτη, με χρήση ψηφιακών πιστοποιητικών, T.A.N. lists ή άλλης μεθόδου), τη μη αποποίηση των συναλλαγών, την κρυπτογράφηση της επικοινωνίας, την ασφάλεια των συναλλαγών (αποδεικτικά στοιχεία επιτυχούς ολοκλήρωσης, αποσύνδεση σε περίπτωση ανενεργού χρήστη, εντοπισμός ύποπτων συναλλαγών κ.λπ.), και τέλος τη λειτουργία των συστημάτων που υποστηρίζουν τις εν λόγω υπηρεσίες σε ειδικές περιοχές του δικτύου που παρέχουν υψηλή προστασία από κακόβουλες ενέργειες εσωτερικών ή εξωτερικών χρηστών.

Γ2. Φυσική Ασφάλεια

Ο όρος «Φυσική Ασφάλεια» αναφέρεται στα μέτρα που πρέπει να λαμβάνονται για την προστασία των συστημάτων και της υποδομής που τα υποστηρίζει, από κινδύνους που προέρχονται από το περιβάλλον. Ανάλυση κινδύνων είναι απαραίτητο να προηγείται της λήψης μέτρων, αφού οι απαιτήσεις φυσικής ασφάλειας δεν είναι δυνατόν να είναι οι ίδιες για όλες τις περιοχές και χώρους που στεγάζουν συστήματα, ούτε και η κρισιμότητα των συστημάτων είναι η ίδια μέσα σε μια συγκεκριμένη περιοχή ή χώρο.

Στα μέτρα φυσικής ασφάλειας πρέπει τουλάχιστον να περιλαμβάνονται:

1. μηχανισμοί ελέγχου φυσικής πρόσβασης (Physical Access Controls). Τέτοιοι μηχανισμοί πρέπει να περιορίζουν, να ελέγχουν και να καταγράφουν, αφ' ενός μεν την είσοδο και την έξοδο του προσωπικού και των επισκεπτών, αφ' ετέρου δε τη διακίνηση μηχανογραφικού εξοπλισμού και αποθηκευτικών μέσων. Μηχανισμοί ελέγχου φυσικής πρόσβασης θα πρέπει να υφίστανται, όχι μόνο σε χώρους που στεγάζουν μηχανογραφικό εξοπλισμό, αλλά και σε χώρους ή σημεία στα οποία υπάρχουν καλωδιώσεις που συνδέουν κρίσιμα συστήματα, υποστηρικτικές συσκευές (π.χ. μονάδες παροχής αδιάλειπτης τάσης, γεννήτριες), μαγνητικά μέσα στα οποία φυλάσσονται αρχεία, κλπ. Επιπλέον, η υλοποίηση τέτοιων μηχανισμών δεν θα πρέπει να περιορίζεται μόνο στους χώρους των μηχανογραφικών κέντρων, αλλά να επεκτείνεται και οπουδήποτε αλλού υπάρχει η σχετική ανάγκη (τοπικά συστήματα καταστημάτων και διευθύνσεων). Το είδος των μηχανισμών ελέγχου που υλοποιούνται θα πρέπει να καθορίζεται από την κρισιμότητα των συστημάτων που καλούνται να προστατεύσουν.

2. μηχανισμοί πρόληψης και αντιμετώπισης καταστροφών από φυσικά αίτια.

3. μηχανισμοί πρόληψης και αντιμετώπισης κακόβουλων ενεργειών (διάρρηξη / κλοπή, βανδαλισμός, τρομοκρατική ενέργεια, κ.λπ.). Οι συγκεκριμένοι κίνδυνοι, όπως και οι κίνδυνοι από φυσικά αίτια, εκτός του ότι μπορεί να προκαλέσουν ολοσχερή καταστροφή των συστημάτων και των δικτύων, είναι δυνατό να διακυβεύσουν τις ζωές του προσωπικού.

4. μηχανισμοί πρόληψης και αντιμετώπισης προβλημάτων από διακοπή λειτουργίας και παροχής υπηρεσιών ή βλάβη υποστηρικτικών συσκευών. Τα συστήματα είναι απαραίτητο να λειτουργούν σε ένα αποτελεσματικά υποστηριζόμενο τεχνικά περιβάλλον.

5. η αποτελεσματική διαχείριση της τηλεπικοινωνιακής και δικτυακής καλωδίωσης για την αντιμετώπιση θεμάτων φθοράς, παρεμβολών και έλλειψης κατάλληλης σήμανσης.

6. μηχανισμοί ασφάλειας φορητών συστημάτων. Η χρήση των φορητών υπολογιστών και οποιωνδήποτε άλλων φορητών συστημάτων θα πρέπει να λαμβάνεται σοβαρά υπόψη στην ανάλυση κινδύνων. Φορητοί υπολογιστές που αποθηκεύουν ευαίσθητα εταιρικά δεδομένα θα πρέπει, αφενός μεν να φυλάσσονται σε ασφαλή σημεία όταν δεν είναι σε χρήση, αφετέρου δε να αποθηκεύουν τα ευαίσθητα δεδομένα σε κρυπτογραφημένη μορφή.

7. η ασφαλής μεταφορά και αποθήκευση των ευαίσθητων εγγράφων και μαγνητικών μέσων. Στην πρώτη κατηγορία ανήκουν οι διαβαθμισμένες αναφορές, οι εφεδρικοί κωδικοί εισόδου των διαχειριστών συστημάτων, τα συνθηματικά των πελατών μέχρι να τους αποσταλούν, η τεκμηρίωση των συστημάτων και εφαρμογών, τα Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή, κα. Στην δεύτερη ανήκουν τα εφεδρικά αντίγραφα αρχείων, το πλαστικό υλικό των καρτών συναλλαγών κ.λπ.

8. η επιλογή και κατάλληλη διαμόρφωση των χώρων με σκοπό την ελαχιστοποίηση των προαναφερθέντων κινδύνων, σε σχέση πάντοτε με τη χρήση για την οποία προορίζονται και την κρισιμότητα των συστημάτων που στεγάζουν.

Γ3. Λογική ασφάλεια

Ο όρος «λογική ασφάλεια» αναφέρεται στο σύνολο των μέτρων που λαμβάνονται για τον περιορισμό της πρόσβασης στους πόρους των συστημάτων (system resources). Ως πόροι των συστημάτων θεωρούνται ο μηχανογραφικός εξοπλισμός, τα δίκτυα, το λογισμικό και τα δεδομένα. Τα μέτρα που υλοποιούν την λογική ασφάλεια καθορίζουν όχι μόνον το «ποιος» ή «τι» (π.χ. πρόγραμμα) θα έχει πρόσβαση σε συγκεκριμένους πόρους του συστήματος, αλλά και το είδος της πρόσβασης που επιτρέπεται να έχει. Τα μέτρα αυτά μπορεί να είναι ενσωματωμένα στα λειτουργικά συστήματα, να υλοποιούνται σε προγράμματα εφαρμογών, σε συστήματα διαχείρισης βάσεων δεδομένων, σε συστήματα επικοινωνιών ή ακόμη να υλοποιούνται μέσω πρόσθετων αυτόνομων πακέτων ασφάλειας.

Για την διατήρηση ενός αποδεκτού επιπέδου λογικής ασφαλείας, κρίνεται σκόπιμο:

(α) για την ασφάλεια των προσβάσεων στα συστήματα

1. να έχουν όλοι οι χρήστες ένα μοναδικό ατομικό λογαριασμό πρόσβασης σε κάθε σύστημα και μόνο για τους πόρους εκείνους που δικαιούνται πρόσβαση, ώστε κάθε ενέργεια να χρεώνεται μονοσήμαντα. Ως εκ τούτου, κοινοί – ομαδικοί λογαριασμοί πρόσβασης δεν θα πρέπει να χρησιμοποιούνται, και όπου αυτό δεν είναι εφικτό, θα πρέπει οι ενέργειες των κατόχων των λογαριασμών αυτών να καταγράφονται και να ελέγχονται σχολαστικά.

2. να υπάρχουν καταγεγραμμένες και εγκεκριμένες διαδικασίες για τη διαχείριση των λογαριασμών πρόσβασης, τον καθορισμό και την αναθεώρηση των δικαιωμάτων που παρέχονται στον κάθε λογαριασμό για όλα τα στάδια της εργασιακής πορείας του ιδιοκτήτη του λογαριασμού (πρόσληψη, μετακίνηση, αλλαγή αντικειμένου εργασίας, αποχώρηση κ.λπ.). Να υπάρχει

διαχωρισμός αρμοδιοτήτων στην έγκριση, υλοποίηση και έλεγχο των προσβάσεων.

3. να καταγράφονται και να ελέγχονται συστηματικά οι ενέργειες που γίνονται με χρήση λογαριασμών πρόσβασης με προνομιακά δικαιώματα, όπως λογαριασμών διαχειριστών συστημάτων και γενικά χρηστών με αυξημένα δικαιώματα.

4. οι λογαριασμοί πρόσβασης να απενεργοποιούνται άμεσα μόλις παύουν να είναι απαραίτητοι ή σε περίπτωση σημαντικής παραβίασης των κανόνων ασφάλειας.

5. να υπάρχει συγκεκριμένη διαδικασία που να προβλέπει τη δημιουργία προσωρινών λογαριασμών πρόσβασης, με καθορισμένο επίπεδο εξουσιοδοτήσεων, για συγκεκριμένες εργασίες ή για περιπτώσεις ανάγκης. Η χρήση των λογαριασμών αυτών θα πρέπει να ελέγχεται σχολαστικά, και μόλις εκλείψει η ανάγκη για την οποία δημιουργήθηκαν θα πρέπει να απενεργοποιούνται.

6. να πιστοποιείται ο ιδιοκτήτης ενός λογαριασμού πρόσβασης, κατά τη διαδικασία εισόδου του στο σύστημα μέσω μιας διαδικασίας υψηλής ασφάλειας (όπως π.χ. κωδικός εισόδου, χρήση «έξυπνης» κάρτας, ψηφιακού πιστοποιητικού κ.λπ.)

7. να αλλάζονται άμεσα οι κωδικοί πρόσβασης που έχουν τεθεί από τις κατασκευάστριες εταιρίες σε κάθε νέο τεχνολογικό εξοπλισμό μετά την παραλαβή του.

8. οι κωδικοί πρόσβασης:

● να δημιουργούνται και να γίνεται η διαχείρισή τους βάσει προτύπων και διαδικασιών

● να είναι δύσκολα προβλέψιμοι

● να διατηρούνται μυστικοί με ευθύνη των κατόχων τους

● να αλλάζουν σε τακτική βάση και οπωσδήποτε την πρώτη φορά εισόδου του κατόχου τους στο σύστημα. Η αλλαγή των κωδικών να επιβάλλεται από το σύστημα, και να κρατείται ιστορικό αλλαγών για την αποφυγή επανάληψης των ίδιων κωδικών, εφόσον αυτό είναι εφικτό

9. οι εφεδρικοί κωδικοί των διαχειριστών συστημάτων ή λογαριασμών ειδικών προνομίων θα πρέπει να βρίσκονται αποθηκευμένοι σε ασφαλές σημείο, ώστε να μπορούν να χρησιμοποιηθούν βάσει ειδικής διαδικασίας σε περίπτωση έκτακτης ανάγκης.

10. όπου κρίνεται αναγκαίο, οι κωδικοί πρόσβασης λογαριασμών ειδικών προνομίων θα πρέπει να μη φυλάσσονται ενιαίοι, αλλά σε τμήματα με ευθύνη διαφορετικών ατόμων.

11. να χρησιμοποιείται - όπου είναι εφικτό - ειδικό λογισμικό διαχείρισης και ελέγχου των προσβάσεων.

(β) για την προστασία των δεδομένων

1. να υπάρχουν επαρκείς ενσωματωμένοι μηχανισμοί ελέγχου (controls) των δεδομένων στα διάφορα συστήματα, και ειδικότερα, στην προετοιμασία, εισαγωγή, και επεξεργασία τους.

2. να υπάρχει καταγεγραμμένη και εγκεκριμένη διαβάθμιση των δεδομένων σύμφωνα με το βαθμό ευαισθησίας τους και να προβλέπονται επιπλέον διαδικασίες ασφάλειας των ευαίσθητων δεδομένων μέσω τεχνικών κρυπτογράφησης ή άλλων μεθόδων προστασίας.

3. για την κρυπτογράφηση:

● να καθορίζεται σαφώς το πότε και σε ποιο επίπεδο γίνεται κρυπτογράφηση

● να χρησιμοποιείται υψηλής ασφάλειας κλειδί κρυπτογράφησης σε όλο το λογισμικό

● να αναπτύσσεται στρατηγική υποδομής Δημόσιου Κλειδιού P.K.I. (public key infrastructure) για τη διαχείριση των ψηφιακών πιστοποιητικών, κυρίως για την επικοινωνία του ΠΙ με τους πελάτες του για παροχή υπηρεσιών ηλεκτρονικής τραπεζικής

● να επιδιώκεται η συμμόρφωση με τους εθνικούς και διεθνείς κανονισμούς και πρακτικές κρυπτογράφησης

4. να γίνονται οι απαραίτητες ενέργειες για τη συμμόρφωση με τη σχετική νομοθεσία και τους κανονισμούς Προστασίας Δεδομένων.

5. να υπάρχει πολιτική σχετικά με την ενημέρωση των πελατών στην περίπτωση διαρροής εμπιστευτικών προσωπικών τους δεδομένων λόγω παραβίασης της ασφάλειας των συστημάτων.

6. για τις βάσεις δεδομένων:

● να υπάρχει ολοκληρωμένη και ακριβής τεκμηρίωση της βάσης που να περιλαμβάνει τουλάχιστον τον λογικό σχεδιασμό, τον φυσικό σχεδιασμό και το λεξικό δεδομένων

● να γίνεται αναδιοργάνωση της βάσης σε τακτά χρονικά διαστήματα

● να εξασφαλίζεται η καταχώρηση μόνο ολοκληρωμένων συναλλαγών (commit / rollback)

(γ) για την προστασία των συστημάτων

1. να υπάρχει εγκαταστημένο κατ' ελάχιστο στα κρίσιμα συστήματα, και όπου αλλού είναι αναγκαίο ειδικό λογισμικό προστασίας από ιούς ή άλλο «κακόβουλο» λογισμικό. Το λογισμικό προστασίας θα πρέπει να ενημερώνεται σε συνεχή βάση και να είναι εγκαταστημένο με τέτοιο τρόπο ώστε να ενεργοποιείται αυτόματα και να μην μπορεί να απενεργοποιηθεί από τους χρήστες των συστημάτων, παρά μόνο από τον αρμόδιο διαχειριστή.

2. να παρέχεται αποτελεσματική προστασία σε ευαίσθητους πόρους των συστημάτων, όπως τα αρχεία συστήματος και εφαρμογών.

3. να συντηρείται αρχείο με το εγκεκριμένο από το ΠΙ λογισμικό

4. να απεγκαθίσταται ή να απενεργοποιείται σε κάθε σύστημα, κάθε λογισμικό ή λειτουργία που δεν κρίνεται απαραίτητη.

5. να ενεργοποιούνται τουλάχιστον οι βασικές λειτουργίες ελέγχου και καταγραφής (auditing & logging functions) σε κάθε σύστημα και να παραμετροποιούνται κατάλληλα σε συνεργασία με τον εσωτερικό έλεγχο.

6. να εξασφαλίζεται όπου αυτό είναι αναγκαίο, κατόπιν σχετικής εγκριτικής διαδικασίας, η συνεχής ενημέρωση των συστημάτων με τις τελευταίες εκδόσεις λογισμικού και ενημερώσεων σε θέματα ασφάλειας, ώστε να ελαχιστοποιούνται οι αδυναμίες και τα τρωτά τους σημεία.

7. να υπάρχουν καταγεγραμμένες διαδικασίες αποκατάστασης της ασφαλούς λειτουργίας ενός συστήματος σε περίπτωση που παραβιαστεί η ασφάλειά του.

8. να προστατεύεται, όσο αυτό είναι εφικτό, το ηλεκτρονικό ταχυδρομείο από πιθανούς κινδύνους αναξιόπιστης γνησιότητας του αποστολέα, υποκλοπής ή και παραποίησης του περιεχομένου, επικίνδυνων προσαρτημάτων, ανεπιθύμητων μηνυμάτων κ.λπ.

9. να υπάρχουν περιορισμοί στις ενέργειες των χρηστών του Διαδικτύου (π.χ. στις προσβάσεις σε συγκεκριμένους διαδικτυακούς τόπους, στη διακίνηση αρχείων κ.λπ.).

10. να γίνεται συνεχής εκπαίδευση και ενημέρωση των χρηστών σε θέματα ασφαλούς λειτουργίας των συστημάτων.

11. να προστατεύονται αποτελεσματικά τα κρίσιμα συστήματα από κακόβουλες ενέργειες εξωτερικών ή εσωτερικών χρηστών. Προς αυτή την κατεύθυνση οφείλουν να υλοποιούνται διάφορες τεχνικές, όπως:

● η χρήση ειδικών συστημάτων (firewalls, filtering routers κ.λπ.), τα οποία, ως σημεία ελέγχου των προσβάσεων, θα ρυθμίζουν και θα ελέγχουν την επικοινωνία από και προς περιοχές του δικτύου οι οποίες είναι συνήθως εκτεθειμένες σε αυξημένους κινδύνους

● η δημιουργία στο δίκτυο ειδικών περιοχών (Demilitarized Zones - DMZ), ανάμεσα σε σημεία ελέγχου προσβάσεων, οι οποίες να λειτουργούν σαν απομονωμένο δίκτυο για τα προσβάσιμα από εσωτερικούς ή εξωτερικούς χρήστες συστήματα του ΠΙ, προστατεύοντας έτσι αποτελεσματικά το υπόλοιπο δίκτυο από κακόβουλες ενέργειες

(δ) για την ασφάλεια της δικτυακής υποδομής και των επικοινωνιών

1. να είναι σαφώς καθορισμένες, καταγεγραμμένες και ελεγχόμενες οι δίοδοι επικοινωνίας (gateways) με εξωτερικά δίκτυα.

2. να εκτιμάται η δυνατότητα κατάτμησης (segmentation) του δικτύου σε ελεγχόμενα επί μέρους υποδίκτυα για τον καλύτερο έλεγχο των προσβάσεων.

3. να μην παραμένουν ανοιχτές λογικές θύρες επικοινωνίας (ports) σε κάθε συσκευή του δικτύου, επιπλέον όσων έχουν καθοριστεί σαφώς ως αναγκαίες για τις υπηρεσίες που υποστηρίζουν και αφού έχει συνεκτιμηθεί ο συνεπαγόμενος κίνδυνος από τη λειτουργία τους.

4. να περιορίζεται και να ελέγχεται επαρκώς η πρόσβαση στις ειδικές λειτουργίες διαχείρισης και ελέγχου του δικτύου.

5. να υπάρχει αποτελεσματική διαχείριση των παραμετροποιήσεων των συσκευών του δικτύου.

6. να υπάρχει η δυνατότητα εντοπισμού από το διαχειριστή του δικτύου λειτουργίας μη εξουσιοδοτημένων συσκευών.

7. να περιορίζονται στα απολύτως απαραίτητα τα σημεία πρόσβασης στο δίκτυο τα οποία βρίσκονται σε χώρους μη ελεγχόμενης φυσικής πρόσβασης, και εφόσον δε χρησιμοποιούνται να είναι ανενεργά.

8. να περιορίζεται και να ελέγχεται συστηματικά η δυνατότητα ασύρματης σύνδεσης χρηστών στο δίκτυο, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων χρηστών σε αυτό.

9. να μην παρέχεται η δυνατότητα απομεμακρυσμένης πρόσβασης στο δίκτυο, και όπου κρίνεται αναγκαία τέτοια πρόσβαση, να καταγράφεται και να ελέγχεται συστηματικά. Ειδικότερα, σε περίπτωση πρόσβασης στο δίκτυο χρηστών μέσω τηλεφωνικής σύνδεσης (dial up), αυτή να πραγματοποιείται κατόπιν διαδικασίας επιστροφής κλήσης (call back) ή άλλης κατάλληλης μεθόδου επαλήθευσης του καλούντος.

10. να χρησιμοποιούνται τα κατάλληλα πρωτόκολλα επικοινωνίας ανάλογα με το είδος των δεδομένων που μεταδίδονται, αντιμετωπίζοντας αποτελεσματικά θέματα διαχείρισης και ασφάλειάς τους.

11. να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα των δεδομένων που μεταδίδονται μέσω του δικτύου καθ' όλη τη διαδρομή τους σε αυτό.

12. να γίνεται χρήση ειδικών εργαλείων λογισμικού για τον εντοπισμό κενών ασφαλείας ή σημείων μειωμένης ασφάλειας στο δίκτυο (vulnerability tests).



13. να υπάρχουν διαδικασίες και συστήματα παρακολούθησης, αποτροπής και αντιμετώπισης προσπαθειών παρείσφρησης στο δίκτυο ή γενικότερα προσπαθειών παραβίασης της ασφάλειας του δικτύου (intrusion detection/prevention systems).

14. να διενεργούνται σε τακτική βάση, από ειδικευμένες εταιρίες, δοκιμαστικές απόπειρες παραβίασης της ασφάλειας του δικτύου (penetration tests), βάσει καθορισμένων σεναρίων, με στόχο την αξιολόγηση της επάρκειας της ασφάλειας του δικτύου.

Γ4. Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή

Το ΠΙ πρέπει να διαθέτει εγκεκριμένα από τη Διοίκηση Σχέδια Συνέχειας Εργασιών (ΣΣΕ) για τα Πληροφοριακά Συστήματα, ενταγμένα στα γενικότερα εταιρικά ΣΣΕ, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους. Επιπλέον, το ΠΙ πρέπει να διαθέτει αποτελεσματικά Σχέδια Ανάκαμψης από Καταστροφή (ΣΑΚ) που θα εφαρμόζονται στις περιπτώσεις καταστροφικών συμβάντων που μπορεί να προκαλέσουν παρατεταμένη διακοπή της λειτουργίας ενός κρίσιμου συστήματος, ή ακόμη και ολόκληρου του μηχανογραφικού κέντρου.

Της δημιουργίας ΣΣΕ και ΣΑΚ θα πρέπει να προηγούνται διαδικασίες ανάλυσης επιχειρηματικών επιπτώσεων (business impact analysis) και ανάλυσης κινδύνων (risk assessment). Βάσει αυτών:

● θα προσδιορίζονται όλες οι κρίσιμες λειτουργίες καθώς και τα συστήματα-πόροι που χρησιμοποιούν

● θα προσδιορίζονται όλοι οι κίνδυνοι που απειλούν τις κρίσιμες λειτουργίες και θα κατατάσσονται σύμφωνα με την πιθανότητα εμφάνισής τους και τις πιθανές επιπτώσεις τους στα συστήματα και τις λειτουργίες

● θα σταθμίζεται το λειτουργικό κόστος από ενδεχόμενη διακοπή των κρίσιμων λειτουργιών και το κόστος ενεργοποίησης του ΣΣΕ & ΣΑΚ για να προσδιορίζονται οι συνθήκες που θα θέτουν σε εφαρμογή το αντίστοιχο σχέδιο

● θα προσδιορίζεται ο χρόνος ανάκαμψης των κρισίμων λειτουργιών - συστημάτων (recovery time) αλλά και το σημείο ανάκαμψης (recovery point), δηλαδή σε πόσο χρόνο και σε ποια εικόνα χρονικά θα επανέλθουν τα συστήματα μετά την ανάκαμψη

Πρώτο επίπεδο εξασφάλισης συνέχειας εργασιών θεωρείται η ύπαρξη σχεδίου λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, συσκευών παροχής αδιάλειπτης τάσης, ηλεκτρογεννητριών κ.λπ., στους χώρους λειτουργίας των συστημάτων.

Με στόχο την εξασφάλιση της γρήγορης και επιτυχούς ανάκτησης των δεδομένων και του λογισμικού, θα πρέπει για τα αντίγραφα ασφαλείας να υφίστανται συγκεκριμένες διαδικασίες:

● δημιουργίας με συχνότητα που υπαγορεύεται από τη κρισιμότητα των πληροφοριών

● ασφαλούς φύλαξης στο χώρο των συστημάτων

● ασφαλούς μεταφοράς και φύλαξης σε απομεμακρυσμένο χώρο των επιπλέον αντιγράφων

● δοκιμών για τη διασφάλιση της ακεραιότητας των δεδομένων

● αρχειοθέτησης με αναγραφή στα μέσα αποθήκευσης του περιεχομένου και του χρόνου αποθήκευσης των δεδομένων

● ανακύκλωσης των μαγνητικών μέσων

Σε δεύτερο επίπεδο, ένα ολοκληρωμένο και αποτελεσματικό ΣΣΕ & ΣΑΚ για τα ΠΣ, συνιστάται:

1. να είναι γραμμένο σε απλή και κατανοητή γλώσσα και να κοινοποιείται επίσημα σε όλο το προσωπικό. Τυχόν διαβαθμισμένες πληροφορίες του σχεδίου (όπως π.χ. κωδικοί, κλείδες ασφαλείας κ.λπ.), θα πρέπει να γνωστοποιούνται μόνο σε εξουσιοδοτημένο προσωπικό.

2. αντίγραφό του να φυλάσσεται σε κατάλληλο χώρο σε ασφαλή απόσταση από το μηχανογραφικό κέντρο.

Ένα τέτοιο σχέδιο θα πρέπει να περιλαμβάνει:

3. κατάταξη των συστημάτων βάση λειτουργικής ανάγκης. Στην κατάταξη αυτή θα πρέπει, μεταξύ άλλων, να αναφέρεται ο χρόνος που απαιτείται για την ανάκτηση (recovery time) του κάθε συστήματος καθώς και η ελάχιστη εκτιμώμενη απόδοσή του μετά την ανάκτηση.

4. τη σαφή ιεραρχική δομή των στελεχών που συμμετέχουν στην εφαρμογή του, τις αρμοδιότητές τους, καθώς και τους υπεύθυνους λήψης αποφάσεων σε κάθε ομάδα έκτακτης ανάγκης.

5. τις διαδικασίες εκτίμησης του εύρους της καταστροφής, με βάση τις οποίες προσδιορίζονται επακριβώς τα τμήματα του σχεδίου τα οποία θα πρέπει να ενεργοποιηθούν.

6. τις διαδικασίες ενεργοποίησης του σχεδίου, ειδοποίησης των στελεχών και κινητοποίησης των ομάδων έκτακτης ανάγκης.

7. τις ενέργειες που θα εκτελούνται σε συγκεκριμένες επείγουσες καταστάσεις, οι οποίες μεταξύ των άλλων θα πρέπει να διασφαλίζουν το προσωπικό σε περίπτωση κινδύνου / καταστροφής (π.χ. φωτιά, σεισμός κ.λπ.).

8. τους εναλλακτικούς χώρους εργασίας των χρηστών, τον εξοπλισμό που θα χρησιμοποιηθεί, καθώς και τις απαιτούμενες προδιαγραφές τους.

9. τις διαδικασίες προετοιμασίας και ενεργοποίησης του εναλλακτικού μηχανογραφικού κέντρου.

10. τα συστήματα του εναλλακτικού κέντρου, την υποδομή τους καθώς και την τοπολογία δικτύου.

11. λίστα προμηθευτών με τους οποίους υπάρχουν συμβάσεις, οι υπηρεσίες που αυτοί προσφέρουν και οι αναμενόμενοι χρόνοι απόκρισής τους σε περίπτωση έκτακτης ανάγκης.

12. τις διαδικασίες που εξασφαλίζουν ότι τα σχέδια συντηρούνται, προσαρμόζονται και ενημερώνονται σε κάθε αλλαγή στις διαδικασίες λειτουργίας του ΠΙ.

13. τις διαδικασίες εκπαίδευσης του προσωπικού σύμφωνα με τις αρμοδιότητες που αναλαμβάνουν κατά την υλοποίηση του Σχεδίου.

14. τις διαδικασίες εκτέλεσης δοκιμών, σύμφωνα με τις οποίες:

- θα προσδιορίζεται η συχνότητά τους (κατ' ελάχιστο μία φορά το χρόνο)
- θα υπάρχουν σαφείς στόχοι εκ των προτέρων, είτε για την εξέταση συγκεκριμένων υποσυστημάτων, είτε για την εξέταση του συστήματος στο σύνολό του. Η εκτέλεση δοκιμών της τελευταίας κατηγορίας συνιστάται να περιλαμβάνει την πλήρη κάλυψη όλων των κρίσιμων λειτουργιών όπως αναγράφονται στο σχέδιο και να κάνει αποκλειστική χρήση του εναλλακτικού χώρου, του εξοπλισμού και των εφεδρικών αντιγράφων
- θα διεξάγονται υπό συνθήκες που θα προσομοιώνουν περιπτώσεις έκτακτης ανάγκης
- θα εξασφαλίζεται η συμμετοχή της Μονάδας Εσωτερικής Επιθεώρησης
- θα συντάσσεται έκθεση των αποτελεσμάτων μετά την ολοκλήρωσή των δοκιμών
- θα γίνονται οι απαραίτητες διορθώσεις στα σχέδια για όλα τα προβλήματα που διαπιστώνονται
- θα λαμβάνει γνώση των αποτελεσμάτων η Διοίκηση και η Επιτροπή Ελέγχου

Τέλος, θα πρέπει:

15. να εξασφαλίζει την αποτελεσματική λειτουργία εναλλακτικού μηχανογραφικού κέντρου, το οποίο θα πρέπει να βρίσκεται σε κατάλληλη απόσταση, ώστε να μην επηρεάζεται από τους ίδιους κινδύνους που μπορεί να πλήξουν το κύριο μηχανογραφικό κέντρο. Το εναλλακτικό κέντρο θα πρέπει να διαθέτει κατάλληλο (εφεδρικό) εξοπλισμό που να παρέχει όλες τις κρίσιμες υπηρεσίες στους χρόνους που έχουν προκαθοριστεί, καθώς και τα εγχειρίδια των διαδικασιών και χρήσης των συστημάτων. Επιπλέον, θα πρέπει να επιτρέπει την απρόσκοπτη χρήση των εναλλακτικών μέσων μέχρι τη στιγμή της επαναφοράς των λειτουργιών στο κύριο μηχανογραφικό κέντρο.

16. να διασφαλίζει τη φυσική ασφάλεια του εναλλακτικού κέντρου, καθώς και ένα βασικό επίπεδο λογικής ασφάλειας κατά την εφαρμογή του σχεδίου.

17. να φροντίζει για την ασφαλιστική κάλυψη του ΠΙ απέναντι σε κινδύνους που είναι δυνατόν να προκαλέσουν διακοπή της λειτουργίας των Πληροφοριακών Συστημάτων.

18. σε περίπτωση που οι χώροι λειτουργίας του εναλλακτικού κέντρου, ο εξοπλισμός ή οι υπηρεσίες παρέχονται από τρίτους:

- να προνοεί, μέσω κατάλληλων συμβάσεων, για την αποτελεσματική συνέχεια των εργασιών σε περίπτωση καταστροφής που θα πλήξει ταυτόχρονα πολλούς οργανισμούς οι οποίοι εξυπηρετούνται από τον ίδιο πάροχο
- να φροντίζει για την ενημέρωση του παρόχου για τυχόν αλλαγές στα συστήματα που πιθανό να απαιτήσουν αντίστοιχες προσαρμογές-ενημερώσεις στα ΣΑΚ

Δ. ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μια αποτελεσματική ελεγκτική λειτουργία για τα Πληροφοριακά Συστήματα θα πρέπει να εστιάζεται στους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία τους, να εξετάζει την επάρκεια των ελεγκτικών μηχανισμών (controls) και διαδικασιών, και να προτείνει, όπου χρειάζεται, τις κατάλληλες τροποποιήσεις. Επιπλέον, θα πρέπει να αξιολογεί το βαθμό συμμόρφωσης με την επιχειρησιακή στρατηγική και τις καταγεγραμμένες επιχειρησιακές πολιτικές, τα πρότυπα και τις διαδικασίες, και να παρακολουθεί το βαθμό συμμόρφωσης με τις διαπιστώσεις των πορισμάτων των ελέγχων. Τέλος θα πρέπει να υπάρχει ολοκληρωμένη εικόνα για τη λειτουργία των Πληροφοριακών Συστημάτων ώστε να δίνεται η δυνατότητα επαρκούς ενημέρωσης σε τακτική βάση της Επιτροπής Ελέγχου.

Για τους λόγους αυτούς, η υπηρεσιακή Μονάδα υ Εσωτερικής Επιθεώρησης θα πρέπει:

1. να διαθέτει την τεχνογνωσία, την ποιοτική και ποσοτική επάρκεια προσωπικού, μέσων και διαδικασιών για τη διενέργεια εξειδικευμένων ελέγχων στα Πληροφοριακά Συστήματα. Η τεχνογνωσία και η εκπαίδευση του προσωπικού θα πρέπει να είναι τέτοιες ώστε να καλύπτονται ελεγκτικά οι τρέχουσες και οι μελλοντικές μηχανογραφικές λειτουργίες του ΠΙ.

2. να καταρτίζει και να υλοποιεί ελεγκτικό πρόγραμμα, το οποίο θα βασίζεται σε ανάλυση κινδύνων που έχει διενεργηθεί στα Πληροφοριακά Συστήματα αλλά και σε ευρήματα προγενέστερων ελέγχων.

3. να ακολουθεί καταγεγραμμένες διαδικασίες σχεδιασμού, οργάνωσης και διενέργειας των ελέγχων, συγγραφής των πορισμάτων καθώς και διαδικασίες επανελέγχου (follow-up). Οι διαδικασίες αυτές, τα κάθε είδους ερωτηματολόγια που χρησιμοποιούνται στους εξειδικευμένους ελέγχους, καθώς και η χρησιμοποιούμενη μεθοδολογία ανάλυσης μηχανογραφικών κινδύνων, θα πρέπει να αποτελούν την επίσημη τεκμηρίωση της λειτουργίας του ελέγχου των Πληροφοριακών Συστημάτων.

4. να παρακολουθεί τα θέματα που αφορούν στα Πληροφοριακά Συστήματα του ΠΙ, ώστε να διαμορφώνει εικόνα για τους κινδύνους που υπάρχουν ή ενδέχεται να ανακύψουν. Για τη διαμόρφωση όσο το δυνατόν πληρέστερης εικόνας, συνιστάται η παρακολούθηση της λειτουργίας των Πληροφοριακών Συστημάτων μέσω ειδικών προσβάσεων, η συμμετοχή στις διάφορες επιτροπές έργων και η ύπαρξη διαδικασιών και μηχανισμών άμεσης ενημέρωσης της Μονάδας Εσωτερικής Επιθεώρησης στις περιπτώσεις εμφάνισης σημαντικών προβλημάτων και εκτάκτων περιστατικών.

5. να κάνει χρήση - ανάλογα με την περίπτωση - ειδικού ελεγκτικού λογισμικού για τον αποτελεσματικότερο έλεγχο της ασφάλειας των συστημάτων και της ακεραιότητας των δεδομένων τους.

6. να συμμετέχει στη φάση σχεδιασμού των συστημάτων για τη διαμόρφωση των κατάλληλων δικλείδων ασφαλείας, των ελεγκτικών αρχείων καταγραφής και αναφορών που παράγονται για τη διευκόλυνση του ελέγχου, καθώς και στη φάση των δοκιμών.

7. να ελέγχει και να αξιολογεί τις διαδικασίες παραγωγής των στοιχείων που υποβάλλονται στη Διοίκηση του ΠΙ και τις Εποπτικές Αρχές, ώστε να διασφαλίζεται η πληρότητα και ακρίβειά τους.

8. να μεριμνά για την άμεση και πλήρη ενημέρωση, στις περιπτώσεις σοβαρών προβλημάτων και έκτακτων περιστατικών στα Πληροφοριακά Συστήματα (περιπτώσεις απάτης, παραβίασης της ασφάλειας σημαντικών συστημάτων, μη διαθεσιμότητας κρισίμων συστημάτων, ενεργοποίησης Σχεδίων Ανάκαμψης από Καταστροφή), της αρμόδιας υπηρεσιακής μονάδας της Διεύθυνσης Εποπτείας Πιστωτικού Συστήματος της Τράπεζας της Ελλάδος, σύμφωνα με τις ισχύουσες διατάξεις.

9. να ελέγχει και να αξιολογεί την επάρκεια και συμμόρφωση με τις διαδικασίες που διέπουν τις φάσεις συνεργασίας του ΠΙ (επιλογή συνεργάτη, σύναψη και τήρηση συμβολαίου, ποιότητα παρεχόμενων υπηρεσιών) με προμηθευτές και παρόχους μηχανογραφικών υπηρεσιών βάσει των προαναφερθέντων στην ενότητα Α3.

10. να επιβλέπει το ελεγκτικό έργο στα συστήματα πληροφορικής σε επίπεδο ομίλου. Για το σκοπό αυτό οφείλει να διατηρεί διαύλους επικοινωνίας με στόχο την αποτελεσματική συνεργασία με τις διοικήσεις και τον εσωτερικό έλεγχο των θυγατρικών και του δικτύου καταστημάτων εξωτερικού. Να αξιολογεί την επάρκεια του ελεγκτικού έργου μέσω περιοδικών αναφορών ή και συμμετοχής του στις Επιτροπές Ελέγχου των θυγατρικών, ειδικά σε αυτές που το μέγεθος και η πολυπλοκότητα των συστημάτων το καθιστούν αναγκαίο. Να αξιολογεί την επάρκεια των διενεργούμενων εξειδικευμένων ελέγχων από εσωτερικούς και εξωτερικούς ελεγκτές. Να προβαίνει σε γενικούς ή ειδικούς ελέγχους ανά περίπτωση, για την κάλυψη των ελεγκτικών αναγκών που είτε δεν καλύπτονται επαρκώς από τον εσωτερικό έλεγχο των εν λόγω μονάδων, είτε κρίνονται απαραίτητοι από τη σχετική ανάλυση κινδύνων.

11. να μελετά, αξιολογεί και εφαρμόζει, όπου κρίνει πρόσφορο, τα διεθνή πρότυπα και μεθοδολογίες ελέγχου Πληροφοριακών Συστημάτων.

Σε ό,τι αφορά στους ελέγχους που ανατίθενται σε εξωτερικούς ελεγκτές, το ΠΙ θα πρέπει να διαθέτει πολιτική για το εύρος και το ρόλο του εξωτερικού ελέγχου στα Πληροφοριακά Συστήματα, καθώς και διαδικασίες αξιολόγησης των προσφερομένων υπηρεσιών. Η πολιτική θα πρέπει να τεκμηριώνει τις περιπτώσεις που ο εξωτερικός έλεγχος δρα, είτε παράλληλα με τον εσωτερικό προσφέροντας μια επιπλέον εξειδικευμένη άποψη, είτε συμπληρωματικά προκειμένου να καλύψει εξειδικευμένες ελεγκτικές απαιτήσεις όπου δεν υπάρχει η δυνατότητα να καλυφθούν εσωτερικά, ή και με τους δύο τρόπους.

Παράρτημα 3

ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΕΚΘΕΣΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΤΟΥ ΣΕΕ ΑΠΟ ΑΝΕΞΑΡΤΗΤΟΥΣ ΕΞΩΤΕΡΙΚΟΥΣ ΕΛΕΓΚΤΕΣ

Η συντασσόμενη έκθεση των ανεξάρτητων εξωτερικών ελεγκτών από εταιρεία ορκωτών ελεγκτών στους οποίους ανατίθεται η αξιολόγηση της επάρκειας του Συστήματος Εσωτερικού Ελέγχου (ΣΕΕ) του πιστωτικού και χρηματοδοτικού ιδρύματος κατά τις διατάξεις της παρ. 4.1 - ενότητα Β2α - Κεφ. IV της παρούσας Πράξης περιλαμβάνει τα ακόλουθα:

Ι. ΑΝΤΙΚΕΙΜΕΝΟ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ ΚΑΙ ΒΑΣΙΚΕΣ ΔΙΑΠΙΣΤΩΣΕΙΣ ΤΗΣ ΕΚΘΕΣΗΣ

1. Η αξιολόγηση της επάρκειας του ΣΕΕ πραγματοποιείται με βάση τις βέλτιστες διεθνείς πρακτικές[1] με στόχο να διασφαλίζονται τα σχετικά με το ΣΕΕ οριζόμενα στην παρούσα Πράξη. Η αξιολόγηση αφορά τη δεδομένη χρονική στιγμή κατά την οποία πραγματοποιείται.

2. Η αξιολόγηση της επάρκειας του ΣΕΕ περιλαμβάνει επισκόπηση:

(i) του περιβάλλοντος ελέγχου,

(ii) της διαδικασίας εκτίμησης των κινδύνων,

(iii) των ελεγκτικών μηχανισμών και δικλείδων ασφαλείας,

(iv) του συστήματος επικοινωνίας και πληροφόρησης, και

(v) του ρόλου και της ευθύνης της Διοίκησης, των εσωτερικών ελεγκτών και του λοιπού προσωπικού.

3. Πριν την έναρξη του έργου, η Επιτροπή Ελέγχου του πιστωτικού ιδρύματος, θα πρέπει να προσδιορίζει τις μονάδες και θυγατρικές που θα συμπεριληφθούν στο έργο (Scoping). Ο προσδιορισμός θα στηρίζεται στη σημαντικότητα κάθε μονάδας και θυγατρικής, καθώς επίσης και σε άλλα ποιοτικά κριτήρια. Το εύρος του έργου (Scope) θα τίθεται εγκαίρως υπόψη της Τράπεζας της Ελλάδος (Διεύθυνση Εποπτείας Πιστωτικού Συστήματος).

4. Με την ολοκλήρωση του έργου υποβάλλεται έκθεση με έκφραση γνώμης του ανεξάρτητου εξωτερικού ελεγκτή ως προς την επάρκεια του συστήματος εσωτερικού ελέγχου όπου θα καταγράφονται οι βασικές

διαπιστώσεις σχετικά με τις ελεγκτικές διαδικασίες και θα περιλαμβάνεται γενική κρίση για την επάρκεια του ΣΕΕ. Θα καταγράφονται τυχόν «ουσιώδεις αδυναμίες», όπως αυτές ορίζονται στα Διεθνή Ελεγκτικά Πρότυπα.

ΙΙ. ΕΙΔΙΚΟΤΕΡΑ ΑΝΤΙΚΕΙΜΕΝΑ ΤΟΥ ΕΡΓΟΥ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ

Στο αντικείμενο του έργου θα πρέπει να περιλαμβάνονται μεταξύ άλλων τα παρακάτω:

Α. Οργανωτική δομή

1.1 Θα εξετάζεται η οργανωτική δομή του πιστωτικού ιδρύματος (οργανόγραμμα, Διοίκηση, Επιτροπές) και θα γίνονται παρατηρήσεις σχετικά με τη διάρθρωσή της.

1.2 Θα εξετάζεται αν το γενικότερο πλαίσιο εταιρικής διακυβέρνησης είναι σύννομο και εξασφαλίζει την έγκαιρη και ακριβή γνωστοποίηση όλων των σημαντικών θεμάτων που αφορούν το πιστωτικό ίδρυμα.

1.3 Θα εξετάζεται η επάρκεια του συστήματος παραγωγής των απαραίτητων στοιχείων και η συμμόρφωση με το κατά περίπτωση αντίστοιχο θεσμικό πλαίσιο.

1.4 Θα εξετάζεται ο ρόλος του Δ.Σ. ως προς τη διασφάλιση της επάρκειας του ΣΕΕ.

1.5 Θα γίνονται σχόλια σχετικά με την τυχόν σύγκρουση αρμοδιοτήτων, τους μηχανισμούς ελέγχου (four eyes principle) και το διαχωρισμό των λειτουργιών πωλήσεων (front line) από τις λειτουργίες επιβεβαίωσης, λογιστικοποίησης και ελέγχου (back office) σύμφωνα με τις διατάξεις της Πράξης.

1.6 Θα εξετάζεται η διαδικασία κατάρτισης του ετήσιου προϋπολογισμού στα πλαίσια της στρατηγικής του πιστωτικού ιδρύματος και οι διαδικασίες που ακολουθούνται σε περίπτωση αποκλίσεων.

2. Βάσει του οργανογράμματος, για κάθε μία από τις μονάδες του πιστωτικού ιδρύματος που θα συμπεριληφθούν στο έργο, αφού γίνει αναγνώριση της υφιστάμενης κατάστασης, θα εξετάζεται κατά πόσο το σύστημα εσωτερικού ελέγχου είναι επαρκές και κατάλληλα τεκμηριωμένο.

Β. Διαχείριση Κινδύνων

1.1. Θα αξιολογείται ο ρόλος της Επιτροπής Διαχείρισης Κινδύνων (αν υφίσταται).

1.2. Θα εξετάζεται κατά πόσο υπάρχουν μηχανισμοί προσδιορισμού, ανάλυσης, ελέγχου και διαχείρισης κάθε μορφής κινδύνου που ενέχει η λειτουργία του πιστωτικού ιδρύματος (σε επίπεδο πιστωτικού ιδρύματος και Ομίλου κατά το κεφάλαιο Ι παρ. 3 του παρόντος παραρτήματος).

1.3. Ιδιαίτερη αναφορά θα γίνεται στην αντιμετώπιση του κινδύνου έλλειψης ρευστότητας σε κατάσταση εκτάκτου ανάγκης.

1.4. Αναφορά θα γίνεται στην ανεξαρτησία, τις αρμοδιότητες και το έργο της Μονάδας Διαχείρισης Κινδύνων και του επικεφαλής της.

1.5. Αν το πιστωτικό ίδρυμα δραστηριοποιείται και στο εξωτερικό, θα εξετάζεται αν υπάρχουν διαφορετικές διαδικασίες διαχείρισης των κινδύνων σε κάθε χώρα.

1.6. Σε περίπτωση σχεδιασμού νέων προϊόντων θα εξετάζεται η διαδικασία αξιολόγησης των κινδύνων πριν την εμπορική τους προώθηση.

2.1. Κατά την αξιολόγηση μονάδων που εμπλέκονται στη διαδικασία παροχής πίστης, στα πλαίσια αξιολόγησης των διαδικασιών, θα εξετάζεται η αντικειμενικότητα της διαδικασίας αξιολόγησης αιτημάτων και έγκρισης πιστωτικών ορίων στους πελάτες, τα εργαλεία που χρησιμοποιούνται για την αξιολόγηση (συστήματα credit scoring ή credit rating), ο τρόπος παρακολούθησης των εξασφαλίσεων των πιστοδοτικών υπολοίπων, η τήρηση των εγκεκριμένων όρων πιστοδότησης, η λήψη μέτρων για τα μη εξυπηρετούμενα δάνεια και η μεταφορά των υπολοίπων σε λογαριασμούς καθυστερήσεων, καθώς και η δυνατότητα παρακολούθησης των κινδύνων σε επίπεδο συνολικού χαρτοφυλακίου του πιστωτικού ιδρύματος.

2.2. Ειδική αναφορά θα γίνεται στις διαδικασίες πιστοδοτικών διευκολύνσεων προς πρόσωπα που διατηρούν ειδική σχέση με το πιστωτικό ίδρυμα και στη διασφάλιση της μη προνομιακής τους μεταχείρισης.

Γ. Λογιστικό Σύστημα

1. Κατά τον έλεγχο των συστημάτων λογιστικής παρακολούθησης των εργασιών θα αξιολογείται η επάρκεια του ΣΕΕ ως προς την κατάρτιση αξιόπιστων οικονομικών καταστάσεων και ως προς την παροχή, μέσω του συστήματος διοικητικής πληροφόρησης του πιστωτικού ιδρύματος (Management Information System) αξιόπιστων οικονομικών στοιχείων για τη λήψη αποφάσεων.

Δ. Συστήματα Πληροφορικής

Θα αξιολογείται η επάρκεια των συστημάτων πληροφορικής έχοντας ως βάση το Παράρτημα 2 της παρούσας Πράξης, και ειδικότερα οι περιοχές:

1. Οργάνωση και Διοίκηση Πληροφορικής.
2. Ανάπτυξη και Προμήθεια Συστημάτων.
3. Λειτουργία Συστημάτων.
4. Φυσική και Λογική Ασφάλεια.
5. Ηλεκτρονική Τραπεζική.
6. Σχέδια Συνέχειας Εργασιών και Ανάκαμψης από Καταστροφή.

Ε. Κανονιστική συμμόρφωση

1. Θα αξιολογείται η Μονάδα Κανονιστικής Συμμόρφωσης (αν δεν υφίσταται, το προσωπικό που έχει επιφορτισθεί με τα σχετικά καθήκοντα) ως προς την ανεξαρτησία της, τη δυνατότητα πρόσβασης σε όλες τις απαιτούμενες πηγές πληροφόρησης, την έγκαιρη και έγκυρη επικοινωνία των ευρημάτων της και την αποτελεσματική ενσωμάτωση των αλλαγών που συντελούνται στο κανονιστικό πλαίσιο.

2. Ειδική αναφορά θα γίνεται ως προς την επάρκεια των διαδικασιών σχετικά με την πρόληψη και καταστολή της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες και της χρηματοδότησης τρομοκρατίας και ειδικότερα ως προς τη διαδικασία ταξινόμησης κατά βαθμίδα κινδύνου των συναλλαγών και των συναλλασσομένων ή συνδυασμού τους.

ΣΤ. Εσωτερικός Έλεγχος

1. Θα αξιολογείται η Επιτροπή Ελέγχου ως προς την ιδιότητα των μελών της, τις αρμοδιότητές της, την εμπλοκή της στη διαδικασία του ελέγχου, την ετήσια έκθεση για την επάρκεια του ΣΕΕ και την ενημέρωση προς το Δ.Σ. Αναφορικά με τη Μονάδα Εσωτερικής

---

[1] *Αναφέρονται ενδεικτικά, τα Διεθνή Ελεγκτικά Πρότυπα (International Standards on Auditing and International Standards of Assurance Engagements), τα Διεθνή Επαγγελματικά Πρότυπα Εσωτερικού Ελέγχου (Standards for Professional Practice of Internal Auditing) και τα υποδείγματα οργάνωσης του Συστήματος Εσωτερικού Ελέγχου COSO (Committee of Sponsoring Organizations of the Treadway Commission)*

Επιθεώρησης, θα εξετάζεται αν διασφαλίζεται η ανεξάρτητη λειτουργία της, εξετάζοντας τη θέση της στο οργανόγραμμα και τη σχέση της τόσο με τη Διοίκηση, όσο και με την Επιτροπή Ελέγχου.

2. Θα αξιολογούνται οι πρακτικές και η μεθοδολογία εσωτερικού ελέγχου, η οποία θα συγκρίνεται με ενδεδειγμένες πρακτικές.

3. Θα γίνεται, δειγματοληπτικά, αξιολόγηση της επάρκειας των εκθέσεων ελέγχου της Μονάδας Εσωτερικής Επιθεώρησης της Τράπεζας και των θυγατρικών της.

4. Θα εξετάζεται η διαδικασία παρακολούθησης της συμμόρφωσης των ελεγχόμενων μονάδων με τις εισηγήσεις των εσωτερικών ελεγκτών.

Ζ. Όμιλος

Για τις θυγατρικές που θα περιλαμβάνονται στο έργο θα αξιολογείται η επάρκεια του ΣΕΕ τους κατά τον ίδιο τρόπο που θα ακολουθηθεί και για το πιστωτικό ίδρυμα.

ΙΙΙ. ΕΥΡΗΜΑΤΑ

Την έκθεση έκφρασης γνώμης θα συνοδεύει αναλυτική έκθεση ευρημάτων.

Διευκρινίζεται ότι η ως άνω έκθεση αξιολογείται από την Επιτροπή Ελέγχου, η δε ποιότητα αξιολόγηση αυτής αποτελεί κριτήριο για τον έλεγχο της εκπλήρωσης των υποχρεώσεων της εν λόγω Επιτροπής από την Τράπεζα της Ελλάδος, κατά τις διατάξεις της παρούσας Πράξης.



ΑΠΟ ΤΟ ΕΘΝΙΚΟ ΤΥΠΟΓΡΑΦΕΙΟ
ΚΑΠΟΔΙΣΤΡΙΟΥ 34 * ΑΘΗΝΑ 104 32 * ΤΗΛ. 210 52 79 000 * FAX 210 52 21 004
ΗΛΕΚΤΡΟΝΙΚΗ ΔΙΕΥΘΥΝΣΗ: http://www.et.gr – e-mail: webmaster@et.gr